THE
KBL
GROUP, INC.

FINAL REPORT TO THE

OFFICE OF TECHNOLOGY ASSESSMENT

ON

AGENCY PROFILES OF CIVIL LIBERTIES PRACTICES

FROM

THE KBL GROUP, INC.

DECEMBER 28, 1984

Karen B. Levitan, Ph.D.
Patrica D. Barth
Diane Griffin Shook

This contractor document was prepared by an outside contractor as an input to an ongoing OTA assessment. It does not necessarily reflect the analytical findings of OTA, the Advisory Panel, or the Technology Assessment Board.

Knowledge Based Living

808 Pershing Drive, Suite 100 • Silver Spring, MD 20910 •(301) 588-4633

J952-43

EXECUTIVE SUMMARY

This report presents the results of an empirical study which profiles the information and technology practices of seven federal agencies/programs as they relate to three civil liberties areas: the collection of personal or company information; the provision of public information; and access to agency decisionmaking.

In the study as a whole, the concept of civil liberties includes freedom of speech and assembly, the right to petition, the public's right to know, due process, equal protection, and privacy. This broad definition of civil liberties is drawn from pertinent statues, regulations, and judicial opinions, as well as the U.S. Constitution. The rights most central to the evaluation of agency information and technology practices are the individual's right to privacy and the public's right to know. An overview of the laws, regulations, and policies governing Federal agency practices which pertain to the rights of privacy and disclosure is contained in Section 2 on the Background.

Criteria for selecting agencies and programs for this study included that they: conduct information practices in all three civil liberty areas of concern; together represent a widespread of agency missions, constituencies, and policy areas; be accessible and willing to provide information to this study; not duplicate other OTA work. Seven agencies and programs were selected for profiling: Department of Agriculture(USDA), administrative functions and its Food and Nutrition Service (FNS); Consumer Product Safety Commission (CPSC) ; Department of Energy, administrative functions and Energy Information Administration; Internal Revenue Service (IRS); Department of Labor, administrative functions and Employment and Training Administration; Small Business Administration (SBA); and Veterans Administration (VA), administrative management.

Data were collected through individual and group interviews, as well as from reviewing and analyzing relevant documentation. The report presents profiles of each agency or program studied, followed by a comparison of agency practices and a discussion of topics for further research. Highlights from these sections are summarized below.

The Technology Environment. In general, agencies are operating in a very mixed computer environment, with mainframes, minis and microcomputers, central, distributed and local management, old and new equipment. The single most important factor in the technology environment is the microcomputer because it puts

the power of information collection, storage, manipulation, processing, retrieval, transfer and printing into the hands of the individual and raises issues of security, productivity and management that have either been dormant or irrelevant before.

Data Protection, Privacy, Confidentiality. Information is collected on individuals and/or companies in all of the agencies which were part of this study. With respect to the impact of information technologies on this area of civil liberties, it is useful to look at: computer matching, FOIA, security, electronic records management, debt reporting and information and data sharing/transfer.

Matching. In 4 of the 7 agencies, (USDA, IRS, Labor, VA), matching has become a routine practice used to initiate, administer, and/or audit programs. In addition, it appears that the lines of responsibility for matching procedures used by state and local authorities for Federal programs do not appear to be clearly defined or documented. Further study is needed to determine the extent to which matching has become routine and and the extent to which responsibilities and procedures have been spelled out for regional, state, local and field offices carrying out Federal programs.

FOIA. The FOIA process appears not to be affected by technology. Agencies follow closely the letter of the law and the focus is on information content. That "content" can be requested whether it resides on paper, microform, computer tape of floppy disk. Information was not sent electronically to answer FOIA requests by any agency studied. FOIA personnel support computerized records because it facilitates their retrieval.

Security. All agencies produce computer security manuals, mostly addressing mainframe and minicomputers, and can control security issues from a central data center. Microcomputer security is seen as a separate issue and was unresolved in all agencies studied. It is important to further document: whether agencies are aware of microcomputer security as an issue; what actions are being taken to understand and address these issues; and whether guidance is needed in the form of standards from NBS or guidelines from GSA.

Data sharing/Transfer. The use of the mail is still widespread in sending documents and computer tapes. Minicomputer networks have been in place for over a decade, and continue to be heavily used. The biggest issue in this area is mainframe-microcomputer downloading/uploading. Once data becomes downloaded, responsibility for security, access, dissemination, maintenance and integrity becomes local and difficult to control. A second transfer area requiring attention is electronic mail. Electronic mail systems generally provide password protection, but

are not considered "secure." In addition, no specific procedures were found which define electronic information exchanges between agency HQ and their regions/field offices and between federal and state governments. Some agencies were found to be under conflicting policies for data sharing; e.g. EIA must share data with the Federal Energy Regulatory Commission. FERC is supposed to make its data public, contradicting EIA's concern with confidentiality. It is suggested that all of these issues be further documented so that policy options can be generated.

Debt Reporting. The Debt Collection Act of 1982 requires agencies to disclose confidential consumer loan information to consumer credit reporting agencies. The micro-mainframe connection makes it easy to download to local credit bureaus where units may not be equipped to deal with considerations of security, access, dissemination and integrity. This is another area which should be further documented so that policy guidance can be developed.

Electronic Records Management. Records management procedures for machine-readable records, especially in records disposition practices and in the definition of "record copy," are missing and needed in all agencies. No agency appeared to know how to manage electronic records. This is significant to civil liberties areas because records management deals with intellectual and physical access procedures, and when properly implemented, provides a tool to deal with security.

Dissemination of Public Information. Public information is disseminated through a variety of media, including hard-copy publications, microfiche, audio-visual materials, and computer and communications technologies. In this area it is useful to look at: printing cuts; dissemination fees; library/information center cuts; electronic dissemination of information; A-76 issues.

Printing Cuts. Four of the 7 agencies reported significant printing cuts (USDA, CPSC, SBA, VA). Interviewees felt their constituencies were negatively affected. At USDA, these cuts were viewed as a stimulus for accelerated applications of electronic information transfer. These indicators need further documentation and analysis.

Dissemination Fees. The policy for charging fees for disseminating information to the public varied by government agency, program, and media. In a few government agencies or program areas where dissemination is seen as integral to mission, information is free, such as at IRS, CPSC. Other agencies charge fees. All electronic dissemination of information has a charge. It is unknown how and by what characteristics constituencies with access to electronic dissemination differ

from those with access to print media. This is an area for further research.

Library/Information Center Cuts. The concerns in this field varied by agency. No agency reported an increase in library/information center activity. Many agencies are contracting out this function. No agency documented the extent of impact to constituencies from library cuts.

Electronic Dissemination of Information. In the majority of agencies, electronic dissemination is in effect or in planning stages. The intent is to provide more efficient and convenient access to information. No agency reported ways they would measure whether they achieved this objective. Activities in this area should be further documented so that policy guidance can be provided.

A-76 Issues. Traditionally, the issues involved in contracting to the private sector have been a matter of policy and budget, rather than of technology. Contracting to the private sector is widespread across all agencies and programs. There is also significant cross-agency contracting, especially to GPO. The extent to which GPO contracts conflict with A-76 policies is an issue for further research. Another issue is the extent to which electronic information dissemination contracts might raise unfair competition in the private sector. This question was raised in USDA when it was preparing and processing an RFP for electronic dissemination of various types of agridata.

Access to Rulemaking. Technology has not altered the number or type of public meetings held. Notice of hearings still are published in the Federal Register and public comments continue to be submitted through conventional means.

TABLE OF CONTENTS

	PAGE
1. PURPOSE AND SCOPE OF THE STUDY	1
2. BACKGROUND	2
2.1 Access to Agency Decisionmaking	2
2.2 Personal Information	5
2.3 Providing Public Information	9
3. METHODOLOGY	11
3.1 Review of the Literature	11
3.2 Selection of Agencies to Profile	11
3.3 Data Collection	12
3.4 Data Analysis and Synthesis	13
4. AGENCY PROFILES	14
4.1 Department of Agriculture	14
4.2 Consumer Product Safety Commission	30
4.3 Department of Energy	49
4.4 Internal Revenue Service (Department of Treasury)	74
4.5 Department of Labor	86
4.6 Small Business Administration	105
4.7 Veterans Administration	130
5. A COMPARISION OF AGENCY PRACTICES	153
5.1 The Technology Environment	153
5.2 Data Protection/Privacy/Confidentiality	153
5.3 Dissemination of Public Information	157
5.4 Access to Rulemaking	160
6. PRESENTATION AND DISCUSSION OF TOPICS FOR FURTHER RESEARCH	161
7. BIBLIOGRAPHY	167
Table 1 - Agencies Selected for Profiling with Criteria Used for Selection	12a
Table 2 - Summary of Findings About Information/ Technology Practices in Three Civil Liberties Areas	153a

Attachment 1 - Interview Protocol
Attachment 2 - Interviewees
Attachment 3 - Agriculture Materials
Attachment 4 - Energy Program Materials

OFFICE OF TECHNOLOGY ASSESSMENT

AGENCY PROFILES OF CIVIL LIBERTIES PRACTICES

1. PURPOSE AND SCOPE OF THE STUDY

This study addresses the civil liberties implications of the use or non-use of information technologies in the procedures and practices of seven Federal agencies profiled by KBL Group, Inc.

In the study as a whole, the concept of civil liberties includes freedom of speech and assembly, the right to petition, the public's "right to know", due process, equal protection, and privacy. This broad definition of civil liberties is drawn from pertinent statutes, regulations, and judicial opinions, as well as the U.S. Constitution. The rights most central to the evaluation of agency practices are the individual's right to privacy and the public's right to know. An overview of the laws, regulations, and policies governing Federal agency practices which pertain to the rights of privacy and disclosure is contained in Section 2, BACKGROUND.

Seven agencies were selected for profiling, based upon selection criteria discussed in Section 3, METHODOLOGY. Descriptions of other criteria and methods are contained in Section 3. Agency practices and their implications for civil liberties were looked at within the context of three areas: public access to agency decision-making; agency acquisition and use of personal information; and agency provision of public information. Agency practices were reviewed to ascertain the extent of use of information technology, and to determine whether the use or non-use affects either the individual's right to privacy or the public's right to information. AGENCY PROFILES are contained in Section 4.

Criteria have been developed for assessing the civil liberties implications of agency procedures. Certain practices have been assigned indicators to represent a likely impact on civil liberties. These indicators have been charted on a comparative matrix of agencies and practices contained in Section 5. Also contained in Section 5 is a discussion of trends.

During the conduct of this study many questions have arisen. These and suggested subjects for further research are contained in Section 6.

2. BACKGROUND: OVERVIEW OF LAWS, REGULATIONS AND POLICIES GOVERNING FEDERAL AGENCY INFORMATION PRACTICES THAT AFFECT CIVIL LIBERTIES AREAS

2.1 ACCESS TO AGENCY DECISIONMAKING

The requirement of providing public access to decisionmaking by Federal agencies can be separated into two aspects: access to information about government activities, and access to the rulemaking process itself. The public's "right to know" about the operations of the government is an essential element of effective public oversight. The availability of government information also serves to protect individual civil liberties, an implication which is discussed in greater detail in 2.2 below. The statutes, regulations, and policies discussed in this section cover both aspects of public access to information held by the government and public access to the actual processes by which agencies promulgate their rules, regulations and policies.

The Freedom of Information Act (5 U.S.C. Section 552, 1966; amended 1967, 1974, 1976 and 1978) has implications for all three civil liberties areas of this study. Certain portions of the act mandate the dissemination of public information. Like the Privacy Act of 1974, FOIA can be a vehicle for obtaining information collected and/or maintained by the government on individuals (discussed in section 2.2 below). The primary purpose of the Freedom of Information Act, however, is to open the records of Federal agencies to public inspection.

Subsection (e) of FOIA defines "agency" to include all independent regulatory agencies, any executive or military department, and any government or government-controlled corporation. Thus all of the agencies profiled by KBL come under the jurisdiction of FOIA.

Every agency is required by the act to actively disseminate the following types of current information: descriptions of its office organization and procedures for interaction with the public; explanations of all formal and informal functions and procedures; and statements of general policies and substantive rules. Agencies are required to make available for public inspection and copying: final adjudicative opinions; interpretations of policy; and staff manuals and instructions that affect the public (National Telecommunications and Information Administration, 1981, p.10). Under FOIA, agencies must provide citizens with all the information they need in order to transact business with the agencies.

The FOIA exempts from disclosure: information that is authorized to be kept secret in the interests of defense or foreign policy; internal agency personnel matters; information specifically exempted from disclosure by other statutes; certain trade secrets; inter- and intra-agency communications that reflect an agency's deliberative process; certain personal information; certain investigatory records compiled for law enforcement purposes; financial regulatory reports; and certain geological and geophysical information (NTIA, 1981, p. 10).

The Administrative Procedures Act (specifically 5 U.S.C. Sections 551 and 553-559, 1966; amended 1976), of which FOIA is a part, also opens the records of Federal agencies, but allows public participation in decisionmaking as well. The agency must provide notice of rulemaking and adjudication to interested parties. Potentially affected parties can participate by submitting written, and often oral comments and by cross-examining witnesses. The APA requires agencies to publish written decisions and a full record of adjudicated proceedings. Citizens may also petition the agency for the issuance, repeal or amendment of a rule.

The use of advisory committees by the Federal Government is another means by which citizens are allowed input into the decisionmaking process. Under the Federal Advisory Committee Act (5 U.S.C. App. Sections 1-15, 1972; amended 1976, 1980 and 1982), commissions, councils, boards, and similar organizations can be established by agencies to provide information and advice. By definition, an advisory committee under this act is composed of members of the public, with one member being an officer or employee of the government.

Except for meetings which can be closed under the Sunshine Act (5 U.S.C. Section 552b, 1976), all advisory committee meetings are open to the general public, and notice of all meetings must be published. Interested persons are allowed to appear before the committee and file statements. Advisory committee records, transcripts, minutes, working papers, reports, and any other documents which were prepared by, or available to, the committee must be made available to the public. The broad categories of documents contained in this portion of the act represent significant access to information held by the government.

The Sunshine Act applies to meetings of the governing boards of collegial agencies, such as the Nuclear Regulatory Commission, as well as to advisory committee meetings. Committee meetings that may be closed under this act are those that fall under the following exceptions: national defense or foreign policy secrets classified as such by Executive order; internal personnel practices of the agency; trade secrets; personal privacy; criminal accusation; law enforcement

investigation; and matters exempted by other statutes. Also exempt from the open meetings law are meetings which would disclose information that would frustrate the implementation of a proposed agency action; or which would lead to financial speculation or endanger the stability of a financial institution. Actually, all meetings pertaining to the regulation of financial institutions can be closed. Among the agencies profiled by KBL Group, only the Consumer Product Safety Commission is headed by a governing body that is required to maintain open meetings under the Sunshine Act.

The Federal Government also grants members of the public the opportunity to participate in decisions of information collection. The Paperwork Reduction Act (44 U.S.C. Sections 3501-3520, 1980) provides that the Director of the Office of Management and Budget may give interested persons the opportunity to be heard, or to submit statements in writing, on whether an agency's request to collect information should be approved (Section 3508).

The movement in government to reduce paperwork was extended to include an effort to reduce or control agency rulemaking. Just before the Paperwork Reduction Act became law, the Analysis of Regulatory Functions Act, (5 U.S.C. Sects. 601-612, 1980) was passed, followed by Executive Order 12291, Federal Regulation Requirements. Both the act and the executive order allow for public access to the rulemaking process to some extent. Each agency is required to publish a biannual agenda of all major rules to be promulgated. The Analysis of Regulatory Functions Act emphasizes the need to fit regulatory and informational requirements to the scale of the entities subject to regulation. To that end, Section 602 requires that small businesses and other small entities likely to be affected by a regulation must be given notice of the biannual agenda (called a regulatory flexibility agenda), either by direct notification or by publication in materials likely to be read by the entities. Comment is then invited on items on the agenda.

A recent proposal of the Office of Management and Budget would allow OMB to screen agencies' regulatory proposals and pre-rulemaking activities before the rules are drafted. The proposals are to be reviewed like budget submissions and compiled for publication as the Administration's Regulatory Program. The stated purpose of the proposal is to clarify administration objectives and priorities for the benefit of Congress and the public. However, there is a concern that OMB's plan would obviate the need for public comment on a proposed rule. (Barringer, 1984, p. A4).

Preliminary regulatory impact analyses are published in the Federal Register, and copies of final impact analyses must be made available to the public. However, under Section 609 of the Analysis of Regulatory Functions Act, if a rule will have a "significant economic impact on a substantial number of small entities," the agency must assure that small entities have been given adequate opportunity to participate in the rulemaking. This access by small entities can be provided by specific notification or publication, as under Section 602, or by the conduct of open conferences or public hearings, or by some modification of procedural rules that will reduce the cost or complexity of small entity participation in rulemaking.

2.2 PERSONAL INFORMATION

The collection and use of personal information by the Federal Government has many implications in the civil liberties area of privacy protection. The Privacy Protection Study Commission found an "...overwhelming imbalance in the record-keeping relationship between an individual and an organization..." and made the following policy recommendations to strengthen the position of the individual in that relationship: 1) to curtail unjustifiably intrusive collection practices; 2) to grant individuals the right to examine and correct information about themselves; and 3) to give individuals control over the disclosure of records pertaining to themselves (The Privacy Protection Study Commission, 1977, p. 30).

For purposes of this study, the definition of personal information has been expanded to include company information. The Consumer Products Safety Commission Act (discussed in the profile of that agency) is concerned with the privacy of business information. The Trade Secrets Act (18 U.S.C. Section 1905, 1948; amended 1980) makes it a crime for any Federal officer, employee or agent to divulge any information considered a trade secret.

The foremost statute affecting agency information handling in these areas is the Privacy Act (5 U.S.C. Section 552a, 1974; amended 1975, 1982 and 1983). Personal information protected by this act includes, but is not limited to, data about an individual's education, financial transactions, medical history, criminal record and employment history. Additionally, the data must contain a name or other individual identifier by which the data may be retrieved from the system of records. The Privacy Act prohibits disclosure of such information unless permission has been obtained from the subject or the disclosure falls within one of the 11 stated exceptions. Disclosure is permitted where the data is to be used as statistical research or reporting; for law enforcement purposes; for routine uses (discussed further below); to consumer reporting agencies; to courts for litigation

purposes; for compelling health and safety reasons; and to governmental bodies such as the Archives, General Services Administration, General Accounting Office, and Congress.

The act allows individuals to gain access to records about themselves, and to request amendment of any errors. If amendment is denied, then a statement of disagreement may be filed by the person affected.

Under the Privacy Act, agencies are required to publish in the Federal Register a description of all their systems of records and the types of individuals about whom records are maintained. They must also notice routine uses of the records, and agency policies and procedures for record storage, access and retrievability.

The act also sets certain standards that agencies must employ to ensure the security, confidentiality and integrity of the data contained in their systems. When records are used to make a determination about an individual, then they must be maintained with such "accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness" in the determination. These standards must also be met before any record may be disseminated. Agency employees designing and maintaining record systems must be trained in these standards and held to rules of conduct based on the Privacy Act requirements.

Agencies are asked to limit their collection of personal information to that "relevant and necessary" to achieve agency purposes, a rather vague standard. There are concerns that the Government's collection efforts may not operate "rationally, efficiently and fairly." (NTIA, 1981, p. 28.)

OMB Circular A-108 speaks to the maintenance of records about individuals. This Circular clarifies the agencies' mandate somewhat by assuring that "...personal information about individuals is limited to that which is legally authorized and necessary, and is maintained in a manner which precludes unwarranted intrusions upon individual privacy." (Transmittal Letter, July 1, 1975, p. 1.) This circular provides guidelines to assist agencies in their compliance with the Privacy Act.

The Privacy Act and the Freedom of Information Act are interrelated, and requests under the acts are often handled by one division within an agency. However, the acts differ considerably in purpose, scope, procedure and effects. The general purpose of FOIA is to strengthen the public's right to know, while the Privacy Act is intended to give the individual better control over information collected about him/herself. All agency records come under the FOIA, but only those within a system of records are covered by the Privacy Act. When a request

is subject to both acts, the effect will differ depending upon whether requesters seek records about themselves or another person. Third party requests must be processed under the FOIA as if the Privacy Act did not exist. If a person asks for his/her own records, the request must be treated under both acts (Saloschin, Newkirk, Gavin and Wood, 1980, p. 46).

The movement toward a reduction in government paper-shuffling affects the collection and use of personal information. One of the stated purposes of the Paperwork Reduction Act is to minimize the cost to the government of information collection, maintenance, use and dissemination. Another purpose is to maximize the usefulness of the information collected (Section 3501). The Director of Office of Management and Budget is to oversee the review of agency requests to collect information, as well as the privacy of records (Section 3504). Before an agency can collect data, it must request approval of the collection scheme from OMB (Section 3511). This act states that OMB may direct agencies to share information that one has collected (Section 3510). Although disclosure is not supposed to be inconsistent with any applicable laws, there is a possibility that the Paperwork Reduction Act may conflict with the Privacy Act in spirit, if not in practice.

A new use of information technology as it is applied to government records is computer matching of one system of data against one or more others. OMB has issued revised guidelines for agencies to follow in computer matching (47 FR 21656, 5/19/82). Computer matches must be listed in each agency's annual report to Congress on uses of information covered by the Privacy Act.

Confidential information is also accessed in agency debt reporting projects. The Debt Collection Act of 1982, P.L. 97-365, amended the Privacy Act and the Federal Claims Collection Act (31 U.S.C.952; 1966) to allow the disclosure of confidential consumer loan information to credit reporting agencies. Furthermore, agencies administering Federal loans included under this statute must collect the applicant's taxpayer identifying number. OMB Bulletin 83-21, issued September 21, 1983, not just allows but requires agencies to report commercial debts and delinquent consumer debts, and to establish procedures for considering credit reports in the approval process for loans, contracts and grants. The Debt Collection Act does require the credit bureau receiving data to comply with the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.) which governs consumer investigative reports. Collection of debts by the agencies and their contractors must be in accordance with the Fair Debt Collection Practices Act (15 U.S.C. 1692 et seq).

The security of an agency's computer systems is vital to the protection of personal and company information confidentiality. Data bases must be kept secure from unauthorized access. The current trend toward downloading of data from mainframes to microcomputers indicates that data integrity must be protected. The Privacy Act is the statutory basis from which data confidentiality efforts must be measured, but it does not contain specific guidelines for computer security. The Federal Information Resources Management Regulations, 41 CFR 201, which became effective April 1, 1984, govern the acquisition, management and use of ADP equipment and software. FIRMR includes a number of provisions that were formerly contained in FPMR, the Federal Property Management Regulations, 41 CFR 101. FIRMR Subparts 201-35.3 and 35.17 discuss the protection of sensitive data and agency requirements derived from the Privacy Act. FIRMR has been modified by a number of temporary regulations and amplified by various bulletins and handbooks (GSA Office of Information Resources Management, 1984, p. 21 and 23.)

OMB Circular A-71 assigns responsibilities for the administration and management of ADP activities. Transmittal Memorandum 1 attached to A-71 provides authority for security checks: agencies must perform assessments of the risk to the agency's missions and objectives should data be improperly disclosed. Circular A-123 implements the Federal Manager's Financial Integrity Act of 1982, which requires agency heads to establish administrative control over all funds and assets of the agency, including loan money. The process mandated by A-123 is a vulnerability assessment rather than a risk assessment. A-123, revised in August 1983, is not explicit about ADP controls, even though computer hardware, software and data bases are surely assets of an agency. The Transmittal Memorandum accompanying A-71 will shortly be revised to link those requirements with procedures instigated by A-123.

Records management is an important part of an agency's entire information handling process. Records Management by Federal Agencies (44 U.S.C. Sections 3101-3107, 1968; amended 1976), and Records Management by the Administrator of General Services Administration (Sections 2901-2909, same dates), both assign responsibility for records creation policies. Concerns are for record quality and quantity. Standards and procedures are to be developed for record maintenance, use and security. While the Administrator of GSA or his designee is allowed to inspect the records and record-keeping practices of an agency, any inspection must be in accordance with the Privacy Act (Section 2906).

Both the FPMR and the FIRMR and their supplemental materials must be consulted to obtain full guidance in electronic records management. Initially, parts of FPMR were relocated in FIRMR. (GSA, 1984, p. 21). Although General Records Schedule 20, in FPMR 101-11.4, indicates that the Federal definition of a record includes all media upon which it might be recorded, the issue is not fully explored. There exists confusion in the field of records management on the definition of a record and a record copy, particularly where both computerized and paper copies are maintained of the same record.

2.3 PROVIDING PUBLIC INFORMATION

All Federal agencies have an affirmative duty to disseminate public information. Information generally regarded as public has been collected and/or developed at Government expense (OMB policy statement, 45 Federal Register 38461, as cited by Levin, 1983, p. 128), and usually as required by public law. Public information is not considered to be classified, personal, or otherwise subject to a Privacy Act or Freedom of Information Act exemption from disclosure. The OMB policy statement further adds: "The distinguishing characteristic...is that the agency seeks...to disseminate such information or otherwise make it available to the public." (Levin, 1983, p. 128.)

The Federal Government as a whole creates and distributes public information under the authority of Title 44 of the U.S. Code. 44 U.S.C. Sec. 1501-1511 (1968, amended 1977), establishes the Federal Register and the Code of Federal Regulations, and describes the content for each publication. The act for Distribution and Sale of Public Documents (44 U.S.C. Sec. 1701-1722, 1968; amended 1977, 1982) sets up the Government Printing Office and defines its responsibilities. Sections 1901-1914 (1968; amended 1972, 1978), create the Depository Library System. Although these statutes were substantially revised in 1968, they are based on acts going back as far as 1895. Even the 1968 revisions occurred well before the current explosion of information technology. There is some concern that these statutes are no longer relevant in today's context (Ad Hoc Advisory Committee on Revision of Title 44, as cited by Levin, 1983, p. 129).

Most of the public information provided for end users is distributed in paper copy or microfiche form (Culnan OTA working paper, p.6). Potential use of new information technologies will have varying impacts on this distribution scheme. Impacts on users could include a problem with access to information due to a lack of money, equipment and/or technical expertise. Information production, on the other hand, could conceivably be impacted by greater efficiency and

productivity,improved retrieval and access, and greater timeliness and flexibility (Culnan, p. 8).

Rather than greater productivity, the recent trend has been toward a decrease in the number of documents published, and attempts to close down bookstores (Smith, 1984, p.278; and Hayes, 1983, p. 330). Numerous publications are never sent to GAO, and many agencies do not comply with depository requirements (Levin, 1983, p. 130). OMB has sought to eliminate many of the more than 500 print shops operated by agencies other than GPO. Because of agency protests, only 101 shops will be shut down, and 10 will be cut back, instead of the original 276 closures planned (Struck, 1984, p. A25).

Another area where policy questions have entered into the dissemination of information is the "fee or free" debate. Government information has traditionally been considered a public good, available free or at minimal cost. The current trend is away from the "free" concept and toward a fee-based distribution system. OMB Circular A-76 mandates encouragement of the private sector to assume an information distribution role. OMB Bulletin 81-16 requires agencies to minimize spending by charging user fees to recover costs. This bulletin also established a moratorium on all new Government publications and mandated the development of guidelines to control the production of existing publications (as cited in Levin, 1983, p.134). The new policy at GPO has been to charge enough to recoup the costs of printing (Struck, 1984, p. A25).

A-76 has resulted in the contracting-out of agency publications, either through the GPO or by the agency itself. GPO contracts out about 73 percent of its work to private firms (Struck, 1984, p. A25). Private contractors have been allowed to copyright the results of Federally-funded research and consultant studies (Levin, 1983, p. 130). The total effect of private sector involvement in the distribution of public information is yet to be discovered.

Dissemination can be required as an element of a larger information handling function, or it can be the sole purpose of some laws and policies. Many of the statutes discussed in Section 2.1 above are access statutes with dissemination aspects. The Freedom of Information Act, Section 552(a)(1-2), describes specific types of information that must be actively disseminated, some by publication in the Federal Register, and some by sale or placement in a reading room. These are the tools the public must use to gain knowledge of, and access to, the procedures agencies use in rulemaking.

Distribution is one of the information handling functions covered by the

Paperwork Reduction Act. Like the collection and use of information, disseminationis an agency activity that must be carefully managed to minimize the cost to the Government (44 U.S.C 3501, 3504, 1980).

A statute which deals primarily with agency information is the Program Information Act (31 U.S.C. 6101-6106, 1982; amended 1983). By its terms, OMB must collect data about all agency domestic assistance programs, such as grants and loans. GSA incorporates the data into the United States Government Assistance Awards Information System. The public is given access to information in the data base through a printed catalog as well as a computerized system. Agencies are responsible for furnishing the current information that makes up the system.

3. METHODOLOGY

The main purpose of this study is to provide empirical evidence of agencies' information and technology practices regarding civil liberties. Given the emphasis on empirical data, the primary methodology of this study involved in-depth interviews with personnel representing current agency structures and functions relevant to information technologies and civil liberty practices. These techniques, along with criteria for agency selection and other aspects of the study rationale, are described in detail below.

3.1 REVIEW OF THE LITERATURE

An extensive review of the literature was conducted to establish a foundation for this study. Most of the results of this review are presented in the BACKGROUND section on p. 2. Aspects of the review which reflect specific agency practices are presented in the agency profiles. The literature review covered the following: acts and regulations; OMB circulars, bulletins, and reports; GAO reports; GSA publications; Congressional hearings; Congressional Research Service publications; NBS publications; and relevant discussions of Federal Government practices in books, monographs, newspapers and journals. These are cited in the attached bibliography.

3.2 SELECTION OF AGENCIES TO PROFILE

In order to meet the objectives of this study and remain within its confines, criteria were developed for choosing agencies. The rationale was based on the following:

- o Ability to meet objectives of this study.
  Agencies must conduct information practices in all three civil liberty areas of concern to this study.
- o Representativeness of Federal agency missions.
  Agencies must together represent policy areas and constituencies of major importance and of wide scope.
- o Accessibility and availability of information.
  Agencies must be: cooperative and willing to participate in this study; small enough to be practically studied within the constraints of this contract.
- o Uniqueness of selection.
  Agencies must not duplicate other OTA contracts in this overall assessment.

Based on these criteria, agencies were simultaneously eliminated and highlighted for profiling. Three OTA meetings with agency representatives also served to narrow the choices. Table 1 lists the seven agencies/programs chosen for the study. As depicted, they all conduct information practices relevant to this study, as well as represent a wide range of important policy issues and constituencies.

3.3 DATA COLLECTION

Data collection was conducted primarily through semi-structured interviews. A protocol was developed to elicit information relevant to the objectives of this study, and used to structure conversations with agency officials. The basic framework of the interview protocol covered the following topics (see Attachment 1 for details of the protocol):

3.3.1 What are the agency's/program's information practices and procedures connected with the three civil liberties targeted in this study?

- o What personal and/or company information is collected? How is it used?
- o How is public access to agency decisionmaking (both rule-making and adjudication) provided?
- o How is public information disseminated? Provide qualitative and quantitative comparisons between dissemination activities in 1976 and at present.

3.3.2 What technology, if any, is involved in each of the three areas?

- o Describe categories of technology.
- o Describe how the use of technology has affected agency information practices. Discuss privacy issues, security, dissemination, access, FOIA.
- o Describe pilot projects, if any, used in collection, adjudication, dissemination.

TABLE 1.

AGENCIES SELECTED FOR PROFILING WITH CRITERIA USED FOR SELECTION

Agency	Personal Info./ Company Info.	Dissemination	Access to Decisionmaking	Constituencies	Type of Agency
1. Agriculture Food & Nutrition National Agric. Library	X	X	X	Consumers Women Children Elderly Schools Food Companies Extension Personnel Farmers Land Grant Universities	Cabinet
2. Consumer Product Safety Commission	X	X	X	Consumers Industry	Independent
3. Energy	X	X	X	Scientists Conservationists Government Officials Industry	Cabinet
4. Labor Employment and Training Admin.	X	X	X	Urban population Workers/labor Unemployed Management Insurance	Cabinet
5. Small Business Administration	X	X	X	Small business Labor Minorities	Independent
6. Treasury Internal Revenue Service	X	X	X	Everyone	Cabinet
7. Veterans Administration	X	X	X	Veterans Students Youth Elderly	Independent

- o Discuss issues that are arising from the use of the technologies in government work.

3.3.3 What plans, if any, does the agency/program have to employ new technologies?

For each agency profiled, the KBL Group interviewed representatives of such offices as: FOIA, Public Information, IRM/ADP/Information Technology Officer, Inspector General, Publications, Information Centers, Records and Administrative Management, and Program Management.

3.4 DATA ANALYSIS AND SYNTHESIS

As information was gathered, profiles of the agencies/programs were developed describing agency practices in the civil liberty areas of personal/company information collection, public information dissemination, and inclusion of the public in decisionmaking.

For each of the three civil liberties areas, criteria were developed for assessing implications and impacts of technologies. The criteria included:

- o types and numbers of constituencies being affected positively and negatively by technology applications and by agency policies in general.
- o changes in types and numbers of public meetings held and comments to proposed rules.
- o changes and numbers of publications disseminated, including educational materials.
- o types and numbers of contracts for information dissemination.
- o numbers of, and reasons for closing libraries/clearinghouses.
- o numbers of marketing documents created/distributed per service program.
- o infringements (or lack of) on personal and company information rights.
- o management procedures in place to handle security/confidentiality with new technologies.

4. AGENCY PROFILES

4.1 DEPARTMENT OF AGRICULTURE

INTRODUCTION

Over one hundred years old, the Department of Agriculture was created by Act of Congress, May 15, 1862, and in 1889 became the eighth executive department in the Federal government. The Department of Agriculture oversees numerous programs to improve and maintain farm production and distribution including: farm income, foreign markets for agricultural products, food subsidies and distribution, production capacity and protection of soil, water, forests and other natural resources, rural development, credit, and conservation programs, agricultural and food science research, agricultural economics, inspection and grading services, and production and product standards. USDA is organized into seven operational divisions, each led by an assistant secretary, and six administrative divisions (See Attachment 1).

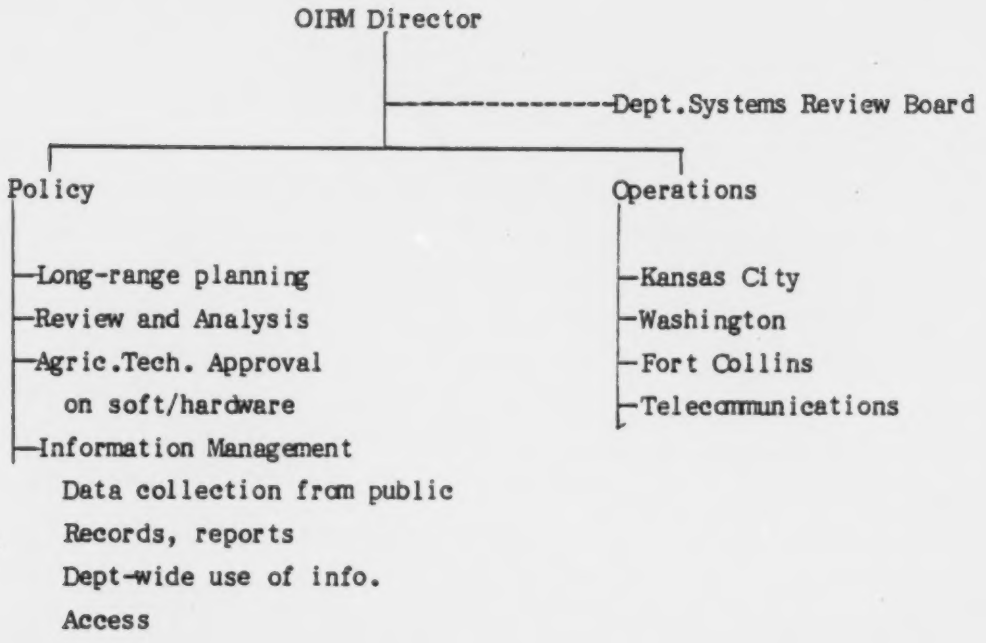
The profile which follows represents only a few offices and one program in USDA: Office of Information Resources Management, Office of the General Counsel, Office of Inspector General, and Food and Nutrition Services under the Assistant Secretary for Food and Consumer Services. The Department is decentralized and distributes its programs into regions and field offices across the country. Computerization follows similar lines, distributed organizationally, functionally and geographically. Because of its age, structure, and functions, USDA appears to be confronting a wide span of issues related to the use of computer technologies. These are presented below.

OFFICE OF INFORMATION RESOURCES MANAGEMENT (OIRM), ADMINISTRATIVE DIVISION

OIRM, Director's Office

The Office of Information Resources Management oversees information, computer, and communications resources for the more than two dozen programs in the Department, as well as for administrative functions. OIRM is organized into two divisions: policy and operations. A Department Systems Review Board serves as an executive secretariat to the Director, and deals with agency-wide systems and

associated policies and decisions.



It is not the responsibility of OIRM to get into the agencies/programs and deal with specifics of information management. It is their responsibility to review agency practices once equipment is in place.

The computer environment for Agriculture is built on a strong mainframe base with progressively large increases of mini and microcomputer acquisitions. For example, Forest Service is acquiring 1,800 minis; Farmers Home 5,000 minis; Agricultural Stabilization Service is buying 2,800 IBM 3600s. There are various estimates of micros in the department ranging from 10 to 15,000.

USDA is pushing "cooperative processing," using mini and microcomputer technologies, and distributed data bases so as to establish conditions which will allow data bases to remain local.

OIRM has not addressed access/security issues in detail on office automation and microcomputer technology.

OIRM, Security

The Department addresses security/confidentiality in Department Regulation 3130-2 on Microcomputer Policy, May 24, 1984 (See Attachment 1). In this regulation sensitive systems are defined as: systems which process national security, personal, financial, proprietary, or market-sensitive data; systems which are

time-critical; systems which affect life-critical situations; systems which have a significant impact on agency operations; or systems whose reconstruction would be difficult or expensive.

If microcomputers are used in a telecommunications environment, departmental security requires special, strict safeguards. Regulations state that sensitive systems shall not be installed in a microcomputer network unless adequate software is acquired or developed and adequate procedures are established to provide the requisite security. Examples of controls which are part of USDA guidelines are: designating one computer to manage the network through use of access control and logging software; and data encryption.

The Department Security staff is fully aware of the decrease in security that comes with increased use of microcomputers. They believe that security is better on floppy disks than on hard disks, and that they will have to rely on personal responsibility and ethics, as well as on management procedures at local levels, to maintain security on this technology.

OIRM, Departmental Systems Review Board (DSRB)

The Departmental Systems Review Board reviews any IRM project with department-wide impact. The project could be related to hardware, software, communications, dissemination, records management, retrieval or other aspects of information management. The following are projects being handled by the review board:

o National Finance Center (NFC) mainframe to micro links. The NFC is implementing FOCUS, a data base/query package which operates on both a mainframe and micro. The intent is to make the personnel/payroll data on their mainframe capable of being downloaded and manipulated by the "owner/creator" agencies. At the present time FOCUS is still being used internally at the NFC and its use by the rest of the Department is under review by the DSRB.

o Use of Electronic Mail for sending information that requires signatures. The Department has installed DEPNET, a communications network on GTE telenet for use throughout the Department. DEPNET provides access to an electronic mail system, which is used mostly informally. Agriculture's policy is not to allow electronic mail to be used for sending policy documents. However, they are currently experimenting with electronic mail for sending time and attendance records. They are testing the procedure of printing the time and attendance records in hard copy, signing the hard copy and keeping that copy with the sender, rather than the traditional route of sending the signed copy to the receiver. With

electronic mail the receiver gets electronic copy with no signature. This is still in test phase.

o Information dissemination. USDA agencies collect or create large amounts of data which have value not only within the Department but also to members of both the public and private sectors. It has been a traditional role of the Department to distribute published data aimed at improving farming practices, increasing sales of agricultural products, and enhancing life in rural America. Information dissemination remains a high priority. Printing budgets have been cut over the past few years, and demands for information are still high. USDA is focusing on technology to provide a more effective way to accomplish this objective.

An interagency project has been established to address electronic dissemination of information. Agencies participating on the policy board are: Agricultural Marketing Service, Economic Research Service, Extension Service, Foreign Agricultural Service, National Agricultural Library, Office of Governmental and Public Affairs, and Statistical Reporting Service with coordination by OIRM. In 1984 USDA released an RFP which resulted in selection of Martin Marietta Data Systems as the network contractor to disseminate agency data. At the time of the award, Agridata Resources, Inc. was concerned that USDA was establishing unfair competition. The Department Systems Review Board met with industry and government representatives to discuss the intent and consequences of this project. The project is not intended for end users, but for brokers who will add value and repackage to meet specific markets.

The contract specification with Martin Marietta specifies two levels of service. The first is primarily to support the information needs of organizations that require data in bulk which will be subsequently enhanced for redistribution. The second level is specifically targeted at USDA end-users who require access to data as specified and managed by USDA and its state level entities and cooperating state institutions. Examples of the reports which will be electronically disseminated through this system are the: Agricultural Marketing Service Market News, Economic Research Service Outlook and Situation Reports, Statistical Reporting Service Crop Reports, and Foreign Agriculture Service Trade Leads. This service is expected to be operational by the end of the first quarter of calendar year 1985.

OIRM, Information and Records Management Division

The Information Management Division develops policies and procedures for USDA management of records, forms, directives, disposition, data administration,

electronic records, and clearance on public use forms. Guidance is needed from GSA on electronic records management. A Task Force was formed last year, which produced guidance which is supposed to be published by GSA. No solutions were devised.

The department developed a locator system with management information about information systems and technologies in USDA. Access to the locator is available to USDA staff, not the general public. It is run off at the Kansas City Computer Center.

OIRM, Washington, D.C. Computer Center

The Washington Center has mission-related data on its systems. Most of the data is obtained through time sharing of big systems (mainframes). With respect to security, it is accomplished through software that has many hooks into the operating systems, providing locks to various parts of the data base. Each agency is supposed to have security officers in charge of data security. The Washington Center is not responsible for "local" data. If a user calls up data and puts it on a floppy disk, it becomes "local" data, no longer within the territory of the Center.

The microcomputer highlights two conflicting themes: productivity vs. security. This conflict should be worked out in agency-wide information policy. The Washington Center director is looking into such policy.

OFFICE OF GOVERNMENTAL AND PUBLIC AFFAIRS (OGPA)

OGPA, Office of Information

Mission and Scope. The Office of Information, a subdivision of the Office of Governmental and Public Affairs, serves as the information interface between the Department of Agriculture and the general public. Some divisions within the Office of Information have an intra-agency service function, such as the Photography, Video/Film, Printing and Publishing, and Design Divisions. The News Division issues all press releases and the Visitors Information Center answers general information questions from the public.

Freedom of Information. The Director of the Office of Information is the FOI Officer for USDA. The actual processing of documents is performed by a Public Affairs Specialist in the Special Programs Division of the Office. Each agency within the Department has its own FOI/Privacy Officer, so the only requests handled by the Office of Information are queries about files held by the Office of the Secretary, and letters that do not or cannot specify the records of only one

agency.

The Public Affairs Specialist determines the agency most likely to possess the records sought by the requester, and forwards the requesting letter to that agency. Requests sent on to other agencies are not tracked by the Office of Information. The Office does not at present have statistics on the number of requests made directly to the agencies; that information is being compiled and will be forthcoming. Informal counts indicate that the number is increasing Department-wide. In the past Fiscal Year, the Office of the Secretary received about 250 requests.

Requests that pass through this Office are distributed as follows: over one-half the requesters are attorneys; the next largest group is businesses; the remainder are members of the general public. Requests for information from the Office of the Secretary's files generally concern controversial topics currently in the news, such as grain exports to Nigeria. Most requests are for statistics, especially economic statistics and crop production figures. Statistical information is generated by accessing the appropriate database and pulling out the data in the requested format. However, most FOIA requests are filled with paper copy materials. There are no current guidelines on charging for computer runs.

Although an FOIA request should not be necessary to obtain statistical public information, most people seem to believe a formal petition is required. If a request for information is received under the Act, it will be processed under the Act regardless of the character of the information sought. Trade associations, on the other hand, do not file formal requests: instead, they contact the appropriate specialist within USDA who is likely to possess the information.

The policy at USDA is to honor requests when possible. Parts of broad requests may be denied. If a query is too broad, negotiating will be done by telephone rather than by sending the letter back to the requester. Proprietary or personal confidential information will be blanked out of records disclosed under FOIA. If a legal proceeding is underway, information pertinent to the suit will also be blanked out.

Appeals are taken up first with the FOIA Officer for USDA, and then with the agency head. In the eight months he has held his current position, the FOIA officer has not received any appeals.

Privacy. The procedures for handling requests for information under the Privacy Act are about the same as under FOIA. This office also serves as coordinator of requests that must be forwarded to other agencies, or that involve more than one agency. The Officer and Public Affairs Specialist provide some guidance to the

other USDA agencies on departmental regulations concerning the Privacy Act. The Department uses the rules and regulations contained in the Code of Federal Regulations as operational policy and procedures in FOIA and Privacy Act matters. There are no additional Standard Operating Procedures or Policy Manual chapters as used in other Federal agencies.

The 1983 Privacy Act Report reveals 198 nonexempt and 45 exempt active systems of records at the Department. No systems were automated in 1983. Out of 155 requests which cited the Privacy Act, 124 were wholly or partially granted.

Training in Privacy Issues. The Office of Information does not see the need for formal staff training since information cannot be released without the approval of the FOI Officer or the Public Affairs Specialist. Training may take place in offices directly responsible for personnel files.

Technology Applications. A manual log system of requests made to the Office of the Secretary is kept, but there are no plans to automate it. There has been discussion about accepting FOIA requests by electronic mail.

The Office of Information as a whole is entering a new phase of computer use. Many personal computers and dedicated word processors have been purchased in the last eight months to serve the distinct needs of each of the five divisions listed above. The Printing and Publishing Division maintains a file of thousands of publications, both active and historic, on 3x5 cards. This filing system will be automated and put up on the mainframe, to be accessed on personal computers in the Division. Publication of documents by this Division will still be hard copy rather than electronic. New graphics equipment was recently installed in the Design Division to be used in computer-enhanced slide processing.

The Video/Film Division expects to go on-line by the end of December 1984 with two-way audio and one-way visual teleconferencing capabilities. Meetings with private industry, such as the Iowa Pork Producers, will be conducted by teleconference. Training segments will be transmitted to USDA field offices. Scientific and technical divisions of USDA will communicate and share information with universities by teleconference. Future uses include dissemination of information to the media and ultimately to rural constituents (farmers,ranchers).

OGPA, Publications Division

Following OMB's Bulletin 81-16 issued in October 1981, there have been severe cuts in the publishing and printing budgets across USDA. In 1981 OMB placed a moratorium on publications. After that time USDA and other agencies had to cut and justify repeatedly. The result has been a cut of 1,400 publications in USDA

with a combination of several hundred others, producing a savings of $3.4 million. There are constituencies which no longer receive information from USDA. For example, various scientists, nutritionists, and members of the general public using educational materials find they can no longer obtain them. Moreover, overall policy in USDA is not to distribute anything free unless distribution is intimately connected to the program and is part of the legislation. Many small publications of 12 to 25 pages are written but not made available through the Superintendent of Documents. Some of these publications used to be distributed through Land Grant Universities and used for educational purposes, but this is no longer the case.

According to the Director of Publications, these cuts have accelerated USDA's search for applications in the dissemination area, but cannot be viewed as an isolated cause for electronic dissemination. Electronic methods do not fill the gap left by cuts in printing because electronic media have attributes which inherently make their use and clientele different from those associated with printed documents. There are many sociological problems still to be resolved in using electronic dissemination as a form for the general public.

More cuts in printing are coming. The Budget Reduction Act, passed last October, includes a $250 million cut in publications and AV material production, as well as a $100 million cut in press and public relations.

OFFICE OF THE INSPECTOR GENERAL

Mission and Scope. The Office of the Inspector General conducts and supervises all audits and investigations relating to the programs and operations of USDA. This Office also has authority over Departmental activities instituted to promote economy and efficiency and to detect fraud.

Computer Matching. USDA took part in the Interagency Audit Project of the President's Council on Integrity and Efficiency. The Final Report of September 16, 1983, shows two USDA matching projects. A comparison of Farmers Home Administration loan recipients with DOD and OPM personnel files identified Federal employees with active farm or rural housing loans. Further auditing revealed ineligible borrowers and delinquent accounts.

Selected Federal personnel files were matched to Food Stamp Program roles in California, the District of Columbia, Georgia and Illinois to identify Federal employees receiving food stamps. Raw hits were researched by program personnel. When overpayments were identified, actions were taken to recoup amounts overpaid

and cases involving potential fraud were referred for investigation.

Although the PCIE project has been concluded, matching programs along similar lines continue to take place at USDA.

Debt Collection Reporting. The 1983 Privacy Act Report for USDA indicates that the agency is in the process of initiating reporting of debt information under the Debt Collection Act.

FOOD AND NUTRITION SERVICE

Mission and Scope. The Food and Nutrition Service (FNS) is a program under the Assistant Secretary for Food and Consumer Services (See Attachment 1). Its mission is to administer the various food assistance programs legislated by Congress. FNS is divided into two main programs with administrative support offices. These are discussed below as related to information and technology practices.

Special Nutrition Programs

The Division of Special Nutrition Programs administers the following food assistance projects: school lunch; school breakfast; child care and family day care homes; summer food program; supplemental food program for women, infants, children (WIC); food distribution; Indian food program; nutrition for the elderly. Under these programs, food assistance support is estimated to provide over 95 million meals a day.

Daily management and operations of these programs requires the collection of personnel information, primarily family size, income, and Social Security numbers. This information is collected at the local level to establish eligibility for program participation. The data is aggregated at the local (including state) level and then passed to the national level.

The collection, manipulation and use of personal information is generally conducted via a three-tiered approach: local, state, and national. State regulations govern districts and local institutions(e.g. schools); national regulations dominate state. Most compliance occurs at the state agency level. In the school lunch program, which includes about 90,000 schools and 20,000 school districts, school district officials review applications and decide on eligibility. They are required to verify a sample of those designated as eligible, and that is when matching occurs. In verifying income, school districts can send applications to welfare offices and match that against their Food Stamp case load. Other matching occurs with wage data and Social Security numbers. Large school districts usually have computers or

access to them, and computerize this process. On the average, at the local level, it is still done manually.

In comparison to Food Stamps, Special Programs have more autonomy at the local level. Those with the most Federal presence include Child Nutrition Programs, School Lunch, Breakfast, and Child Care. WIC, Needy Indians, and the Commodity Distribution Programs have more local autonomy. Those with the most autonomy include Temporary Food Assistance and Elderly Feeding. WIC has the tightest security on records.

Food Stamp Program

The Food Stamp Program is administered primarily at the state and national levels. In states where the program is locally administered, the states still control policies and procedures. They must collect personal information for eligibility decisions, including: name, birth date, Social Security number, income, members in household and their income and assets, household expenses (rent, mortgage and utilities). This information is stored as the individual's case record. State welfare employees and the individuals themselves, have right of access to these records. They are kept in the local or state computers.

To determine recipients' eligibility, Food Stamp information is matched against any of the following: unemployment compensation, birth certification, Social Security Administration (for benefits and wages), Veteran Administration data, State employment records, Department of Motor Vehicle Records, and bank savings (Massachusetts). This is called front end matching or "means" testing. In these instances, potential recipients are made aware of the process and must sign forms to allow verification to proceed.

Other matching is done for quality control purposes, to determine if the rules and regulations are being followed. This is matching after eligibility has been determined—post verification—and the recipients are generally not made aware of this process. These checks are done periodically to determine changes in the household status.

Restraints on the use of data are based on statutory regulations from the national office. Most restrictions focus on disclosure limitations in Food Stamp legislation. The Federal government has regulatory authority to withhold administrative funds until problems are corrected. They have never had to withhold on a disclosure case.

One quality control program is maintained at the national level, the Disqualified Recipients' Information Program. Those food stamp recipients who are

transmitted to FNS Regions and Headquarters. States send to FNS Headquarters through the regions the name, Social Security number, date of birth, number of disqualifications, effective date of disqualification and length of disqualification for each disqualified recipient. Each State can get, upon request, a report from the national data base on those disqualified. Each State can also get a tape listing disqualified persons to check against its current food stamp recipient list. This information program is relatively new, and no statements can yet be made on its effectiveness or problems.

Matching continues to receive emphasis in various pieces of legislation. Under the Deficit Reduction Act, passed last year: States are required to continue wage and Social Security matching under the food stamp program; the 12 or 13 States without matching are required to set up such matching by January 1985; and States have been given access to IRS data on interest income claimed by food stamp recipients.

The majority of States use a central computer to process food stamp data. There have been movements to coordinate welfare information management so as to share computer resources. FNS has cooperated with HHS and Social Security. Staff at State welfare agencies are trained at those locations. Training about privacy/confidentiality is a state responsibility. Generally states are sensitive to privacy issues. Computers supporting the FNS program are not networked. Information is transmitted mostly on paper, sometimes on tape, and processed in batch mode. There are no plans to network food stamp data; it is too expensive.

As part of the program, information about eligibility and program benefits is made available, primarily in pamphlet form. Pamphlets are printed stating rights and responsibilities. The national office prints these pamphlets. There have been no cutbacks in printing. State costs are matched at the national level on a 50/50 basis, or pamphlets are made available at cost. Infrequent meetings at regional levels are sometimes held to obtain input from advocacy groups.

FNS, Rulemaking

Rules that govern the food stamp and special food programs are cleared through a central office. A computerized tracking system is used to monitor progress on clearance. They are then published in the Federal Register and open to comments.

FNS, Administrative Management

In comparison to other agencies, FNS does not receive many FOIA requests—approximately 150 per year. Requests come mostly from advocacy groups,

then lawyers, and finally, from individuals. People seeking information on FNS programs generally go through the States first, since the programs are state assistance programs.

With respect to ADP status, there are two types of systems: one to handle programmatic delivery, and the other to handle internal computing for FNS operations. The first category is under state responsibility. OMB says that the agencies can only provide guidelines. Therefore, FNS cannot and is not orchestrating a national system. States are requested to submit advanced planning documents in order to get funds. In order to manage effectively, they must rely on a partnership with the states, which will evolve through new inter-institutional procedures. A current review of state systems is in process by the Inspector General.

ADP systems internal to FNS are mostly operated in batch mode. The goal for 1985 is to acquire 120 to 200 microcomputers. A security section will be responsible for working out procedures for micro utilization. At the present time, FNS controls hardware and software acquisitions and eligibility for getting a machine.

DATA ANALYSIS AND SYNTHESIS

1. Constituencies Affected. In both the data protection/privacy area and information dissemination issues, changes are occurring which affect large constituencies. For example, computer matching has become a common administrative tool in FNS in the various food assistance programs, and many identifiers are used to determine eligibility and provide quality control to these programs. With the increased use of computers at local and state levels, the potential for privacy infringement increases even more. However, few infringements were reported during the data collection phase of this study. Another constituency to watch in the data protection/privacy area includes the overall employees of USDA and the transfer of their payroll and personnel records across mainframe to micro links. With respect to dissemination, it is clear that the severe cuts in printing and publishing at USDA have reduced access to information by the general public. Given the online and computer costs, as well as the educational background needed to use electronic systems effectively, it seems clear that a new constituency will develop around USDA's electronic dissemination project.

2. Public Meetings and Comment on Proposed Rulemaking. In the few interviews

conducted about this topic, there was no indication that computers and other information technologies are being used, or will be used in the future. Cost is the primary reason cited for not using technology to improve this area.

3. Dissemination of Publications. USDA has cut back severely in the dissemination of printed materials and is beginning to take new directions with electronic dissemination. It is now their policy not to disseminate anything for free, except in rare circumstances where dissemination is integral to the program's implementation. In a new contract recently awarded to Martin Marietta Data Systems, several "data-based" publications will be disseminated through an online service. The project is still in design phase, so it is too soon to determine precisely its effectiveness or impact, and should be monitored over the next few years to document its differences from hard copy, its difficulties and successes.

4. Contracts for dissemination. Aside from the Martin Marietta contract, this topic was not discussed at length during the study. Specific data on this topic per se is not kept by contracting officers, but must be derived from program managers. USDA's electronic dissemination of information RFP and award bears watching because it generated a great deal of controversy from the private sector. Small agri-data firms objected to the award, fearing a monopoly and unfair competition. The Information Industry Association raised the issue of government involvement as a whole. Yet the project proceeded and is underway. More information is needed on issues in this area. Given the use of technology for dissemination, it would be interesting to determine whether dissemination contract awards have changed in the sense of going to computer firms rather than to publishers, printers or writers.

5. Library Closings. Not Applicable/Not Found

6. Marketing. According to the FNS interviews, documents to explain and sell food assistance programs are still being produced with no difficulties or cuts in the budget. The Federal Government provides these documents at cost to state participants. From the publications available in the program offices, newsletters are being developed to communicate program activities and publicize commendable behavior of State and local administrators. Whether this would be true of other offices in USDA could only be determined through further study.

7. Personal and Company Information Rights. A great deal of personal and company information is collected at USDA to administer its programs and services. Personal information identifiers on birth, name, residence, wages, households, interest on income, motor vehicle registration, Social Security number and other identifiers provide criteria for eligibility and quality control. Individuals whose

identification is being manipulated on computer are told about it if it deals with eligibility, but are not made aware of the manipulation if it occurs after eligibility has been determined, when used for maintenance and validity. Company and personal information is collected on farms and farm cooperatives, inspection services, and production plants in other programs in USDA, but these were not part of the current study.

The electronic transfer of employee payroll and personnel records which are kept at the National Finance Center will soon be available to offices throughout USDA. Data protection issues are currently under study by the Departmental Systems Review Board.

The Departmental Systems and Review Board is experimenting with electronic transfer of time and attendance cards as a way to define procedures for handling the signature chain when using computer/communications technologies. At present, the procedure is to print hard copy at the place of creation/origin, sign hard copy and retain signed copy at place of origin while sending electronic records unsigned to place of destination. This procedure has not been in effect long enough to determine full consequences of its implementation.

8. Security Procedures. Security of information and of equipment is a major concern at the Departmental level and in FNS. Extensive guidelines have been written and distributed by the OIRM on security options for mainframes and mini computers. Security of information on a micro is admittedly an unresolved problem in USDA. Their overall policy is: "when in doubt, do not put the data on the micro." The issue of downloading sensitive data from mainframe to micro is receiving attention throughout USDA. The Director of the Washington Computer Center made it clear that once the data is downloaded, security becomes a local responsibility and policies defining access become central. Given the decentralized nature of program implementation, which involves numerous Federal-State relationships as well as field-HQ interactions, adequate access and data protection procedures for the various working environments is taking extensive effort to resolve.

TOPICS FOR FURTHER RESEARCH

This profile barely scratched the surface of information activities in USDA, and yet numerous issues have been raised which warrant further attention.

Several current projects which reflect USDA's approach to electronic media

procedures should be monitored and viewed as prime examples of how to handle changes brought about by the technologies. These include:

o Departmental Systems Review Board's (DSRB) study of the National Finance Center's implementation of the FOCUS data management software package for the mainframe and PC;

o DSRB's pilot test of electronic transfer of time and attendance cards

o Electronic dissemination project with Martin Marietta (for A-76 issues, as well as for insight into new, computer-literate, economically capable constituencies);

o OIRM efforts to develop machine-readable records management procedures;

o DSRB and agency committee efforts to define responsibilities and procedures for data security at the local level in using microcomputers

o FNS efforts to define and implement Federal-state "partnerships" in information transfer and management.

The topic of Federal-State interactions in implementing Federal programs at local levels is one which deserves considerable attention. The use of information technologies to enhance the many and complex relationships between Federal and State governments has not been studied or documented. Such research is needed to get at the underlying issues inherent in the use of technologies in these programs. Along a similar line, it would be valuable to investigate national-regional-field office communication and information transfer in order to identify management areas or security procedures that need to be addressed in light of the new technologies.

Conclusions and generalizations about the impact of information technologies on civil liberties in USDA cannot be made without accounting for activities in many other offices of the department. To further substantiate this profile we recommend continued study along the following lines:

o To determine the effect of printing cuts on the general public, investigate practices in: Economic Research Service, Statistical Reporting Service, World Agricultural Outlook Board, Human Nutrition Information Service, Office of the Consumer Advisor, Extension Service, National Agricultural Library; also explore their relationships with NTIS and GPO to determine the extent to which publications from their programs are made available, on the one hand, and actually purchased, on the other hand.

o To determine the extent to which research results are being archived and disseminated, analyze the information flows of research conducted by Forest Service, Soil Conservation Service, Agricultural Research Service, Cooperative State

Research Service, National Agricultural Library, and Human Nutrition Information Service.

o To determine whether printing cuts have accelerated electronic dissemination applications in the Department, discuss issues with persons in publications and public relations, as well as collect data from the programs listed in the paragraph above.

o To determine uses of personal/company identifiers, examine programs under the Assistant Secretaries for Marketing and Inspection Services, International Affairs and Commodity Programs, and Small Community and Rural Development.

o To identify creative uses of computer technologies and potential, new issues, study the plans and practices in the research-oriented programs (e.g. Forest Service, Soil Conservation Service, Agricultural Research Service).

o To explore Federal-State uses of information technologies, study the programs under the marketing and inspection services, as well as the Cooperative State Research Service and Extension Service.

4.2 CONSUMER PRODUCT SAFETY COMMISSION

INTRODUCTION

The Consumer Product Safety Commission is an independent Federal regulatory agency established by the Consumer Product Safety Act (15 U.S.C. 2051 et seq., 1972, amended 1976, 1978, 1981 and 1983). In addition to the authority established under that act, the Commission is responsible for the implementation of four other statutes, none of which are relevant to the scope of this study: the Flammable Fabrics Act, the Poison Prevention Packaging Act, the Federal Hazardous Substances Act and the act of August 1, 1956, which prohibits the transportation of refrigerators without door safety devices.

The agency mission is to help protect the public from unreasonable risks of injury associated with consumer products. To that end, the Commission engages in the following varieties of information gathering, disseminating and regulatory functions.

Information on consumer product-related injuries is collected and maintained. A sampling of accidents is investigated. Research on product hazards is conducted. Publications are created and distributed to the public. Manufacturers are required to report defects in products that could create substantial product hazards (Consumer Product Safety Act, Section 15 (b)). Corrective action or recalls can be required for substantially hazardous products already in commerce. Other regulatory activities include the development of voluntary safety standards, the promulgation of mandatory standards, and the banning of hazardous products.

Except for the data collection of the National Electronic Injury Surveillance System and related files created and maintained by the Directorate for Epidemiology, the Consumer Product Safey Commission has not automated its information handling procedures. The information technology that is presently in use and planned for use in the near future is primarily employed as a means of internal paper tracking. Public access to rulemaking, and the dissemination of public information, are still handled by traditional means. These and other issues are described in detail in the following profile. Organizational units are first described, followed by an analysis of civil liberty implications.

OFFICE OF THE SECRETARY

Mission and Scope. The Office of the Secretary sees that notices of proposed rulemaking and of meetings of the Commission are published, although the Office of the General Counsel (OGC) actually prepares the notices as well as the rules. The office logs in comments made on proposed rules and makes them available to the necessary program staff. There is a manual numbering system for each of the five CPSC administers. At the reading room downtown under the Secretary's jurisdiction the documents are kept in notebooks and indexed by commentor and date of receipt. There are no immediate plans to automate this system—there is no great burden as there are only 15 rulemakings per year, and only 8-10 comments per each rulemaking. Likewise, there are no plans to implement electronic mail for comments. There would be greater convenience for commentors far away, but no significant saving of administrative burden.

This office transmits the decision packages and controls the voting process. The packages are compiled by the technical staff and commented upon by the Office of the General Counsel. The OGC decides what type of vote is appropriate: a ballot for non-controversial measures, or the finalizations of matters upon which the Commission has already met; an agenda meeting for controversial matters. Often the Commissioners will decide to meet even if OGC believes a ballot is sufficient. There are about 250-300 ballot votes per year. These are usually "mini-issues". A lot of public agenda meetings do not approach rulemaking, so the only notice publicized is that required by the Sunshine Act.

The Commission sometimes acts on petitions from outside sources—about 6-8 petitions per year. Normally all matters flow from the work of the staff, which has previously been approved in an operating plan set up annually by the Commission. The operating plan may be adjusted at the mid-year review. In the operating plan, the Commission outlines the areas for staff concentration for the year. When they feel that sufficient information exists for rulemaking, the matter will be presented for action by the Commission. The staff may only give status reports about ongoing research and not approach the stage of requesting a rulemaking for some time. Many matters never become the subject of rulemaking.

The Commission meets once or twice a week, except for holidays or if one or more is traveling (they travel to give speeches and press conferences). They have never met by video conference because of the expense. If there is time urgency,

and there is split voting (all are needed to arrive at a decision), then they may allow one Commissioner to vote by telephone. This has happened only rarely.

Dissemination. All the materials are published by the Government Printing Office. The Secretary's role is purely administrative—the office manages a contract with the D.C. Association for the Retarded at St. Elizabeth's Hospital. They warehouse the materials, maintain a monthly inventory, stuff envelopes, and box and assemble packets. The Outreach Office and the Public Affairs Office develop materials, have them printed, and generally maintain programmatic control. The Secretary's office also has purely administrative control. It oversees the FOI Office,the Hotline, and a Correspondence Office. The correspondence unit opens and sorts mail requests for documents. These are batched and sent to Automatic Data Processing for label generation. The Hotline is now able to enter addresses and information requests online. Hotline requests for information are also sent to St. Elizabeth's.

Plans for Automation. The Hotline will shortly be able to retrieve information online, such as press releases going back six months. The Director for Compliance is putting an index to all compliance files online. In addition to the information requests mailing list, the hotline also enters complaints online.

Access to Rulemaking. The Office of the Secretary publishes a Public Calendar which covers two weeks of meetings of the Commission. This will be put online soon so that the information can be put into a different format for the annual report. This is Commission policy, not a Sunshine Act requirement. After meetings, logs are created of about 1 to 1-1/2 pages and placed in the public reading room, filed chronologically. In the annual report, meetings are indexed by names of persons with whom the Commission met.

Other Changes to the Agency since 1976. Sec. 15(b) of the CPSC Act requires manufacturers and distributors to report to CPSC products which might be hazardous. Each manufacturer has one designated officer who informs the CPSC Compliance Division by telephone and a followup letter. About 8-10 reports per week are received. Section 15(b) conflicts with FOIA--in that if a manufacturer has reason to believe its product could create a substantial hazard and reports this to CPSC, then there is a potential recall situation. There are frequent FOI requests for product hazard information that may have been voluntarily submitted under 15(b), so the CPSC Act was amended to say that 15(b) information is not releasable unless certain restrictive requirements have been met. The issue becomes a policy question—whether certain information should be considered as having been submitted under 15(b).

The office also has a docket control function: it acts as aclerk of the court in matters that go before the administrative law judges. CPSC borrows law judges to hear compliance cases where the dispute centers on the remedy, or on whether the product is hazardous. The Compliance Division has its own attorneys. The Commission acts as the final appellate court.

OFFICE OF THE GENERAL COUNSEL

Mission and Scope. There are 20 attorneys in the Office of the General Counsel. All deal to some extent with FOI, but five of them concentrate particularly on this issue. Each staff member has his/her own style in handling disclosure questions. Some attorneys deal with two sections of the CPSC statute primarily—Sections 6(a) and (b).

1. Section 6(a) prohibits the disclosure of trade secret information (note also the Trade Secrets Act which provides criminal penalties). CPSC honors approximately 80 percent of the requests of manufacturers claiming that information contains trade secrets.

2. Section 6(b) requires CPSC to take "reasonable steps" to assure the accuracy of information containing the identity of the manufacturer before disclosing it. CPSC honors roughly 50 percent of requests from manufacturers claiming that information from which their identity may be discerned is inaccurate and requesting it not be disclosed.

Negotiation Standards. There is "a lot of dickering overminutiae," according to one attorney. If the manufacturer produces test data to show their product was not at fault, and it is conclusive, then CPSC will not disclose. If the manufacturers data is not conclusive, the disclosure will contain both industry and CPSC data, or the office may disclose the information, but add many disclaimers. When the requester asks for information about a product supposed to have caused a mishap, and the data connecting the product is not really relevant (e.g., the product was at the scene of the fire, but was not proven to be the cause of it) then they will withhold the data as not responsive to the request. If the manufacturer claims the product has been misidentified by the consumer, they will not disclose the requested data because the manufacturer has created a reasonable doubt.

CPSC attorneys in the Office of the General Counsel deal primarily with private counsel for plaintiffs, manufacturers, and trade associations. Some private individuals do request data. Attorneys seeking information usually represent either

plaintiffs in product liability cases or trade associations. Those who seek to prohibit disclosure generally represent manufacturers. Most requests come in under FOIA, but some attorneys will call and ask for documents on an informal basis. Staff will release information as a professional courtesy, as long as it is not a disclosure subject to 6(b).

Attorneys also call about depositions—they will try to make expert witnesses of technical people. Sometimes they will make an FOI request, and then use the information gained to identify investigators to depose. When CPSC sends documents out to manufacturers for notice and comment under 6(b), then attorneys will seek discovery from the manufacturer.

Once a disclosure determination is made, it goes to the Assistant General Counsel for approval, and then on to the FOI office for disclosure.

DIRECTORATE FOR ADMINISTRATION OF THE CONSUMER PRODUCT SAFETY COMMISSION

Mission and Scope. The Directorate for Administration of the Consumer Product Safety Commission oversees the basic operation of the agency, including functions such as procurement, personnel, contracts and budget. One staff person within the Administration Directorate is in charge of information resources management and security.

Since January of 1984 the Commission has been undergoing an extensive records management and security review. A risk analysis performed by private consultants in 1983 was reviewed by CPSC staff and used as a starting point for their own analysis. A high level steering committee has been established to ensure that the analysis will be carried out in every directorate.

Each directorate is to be studied individually. The procedures of the Directorate for Compliance have been reviewed, and new guidelines developed. Reviews of the Office of the Secretary and the Directorate for Epidemiology are to be completed in about six months.

Criteria have been developed to identify the level of classification of documents and computerized data. The three levels of classification, in ascending order of degree of security, are: 1) controlled; 2) restricted; and 3) confidential business information. Information which is considered controlled is information that generally would be subject to the Privacy Act, such as personnel data. Restricted information includes product information from which the identity of a manufacturer

could be ascertained (CPSC Act, Sec. 6(b)); litigation strategy; and sensitive staffing and budget information. CPSC uses the definition of restricted information from the National Archives Act. Confidential business information consists of trade secrets and other proprietary information as defined by the Trade Secrets Act and Section 6(a) of the CPSC Act.

There are two other classifications of information not ordinarily employed that are reserved for data obtained from the Environmental Protection Agency. Material transmitted from EPA under the Toxic Substances Control Act (TOSCA) is maintained under EPA security procedures and classified as Option 1 or Option 2.

Each level of classification has specific security control—physical control for the documents and Automatic Data Processing controls for the computerized files. At the highest level of classification, TOSCA Option 2, the data cannot be computerized or electronically transmitted at all.

Classification levels were arrived at by analyzing thedegree of risk to agency missions and objectives if information of each type were to be wrongfully disclosed. CPSC goals that were considered in the analysis were: protection of the public, maintenance of public trust, enforcement of the laws entrusted to CPSC, and the protection of trade secrets.

The OPM Federal Personnel Manual 732 was also used in the development of security standards.

Guidelines are being developed in draft form for each directorate as their procedures are reviewed. After the review is completed the guidelines will be formalized into Standard Operating Procedures.

Staff Training. A manual on Information Resources Management is being developed. The chapter on security is concerned with the protection, integrity, and sensitivity of data. All staff persons up to the Commissioners will be required to read pertinent chapters, take a self-test, and sign a training certificate.

Telecommunications represents the biggest gap in security, but CPSC does not currently employ this means of communication. In December of 1984, the New York and Dallas field offices will be able to communicate electronically with the Compliance Directorate at the National CPSC office. The goal is for maximun data sharing using the new work stations. ADP controls, such as password and access protection, will be implemented. Extremely sensitive data, such as the EPA TOSCA information, will continue to be sent by courier, since there are no funds to allow for encrypting. Information classified up to restricted will be sent electronically. Some confidential business information will be transmitted, but none containing

formulas.

The workstations will also be used for information access throughout the agency here. In a year's time the office hopes to have completed a survey of all data held by each directorate. All databases will be linked and hard copy located through the new keyword system.

The new system is currently used by the FOI Office to locate files in the Compliance Directorate. Files that are in the compliance process are kept on shelves in a temporary storage area. When a product code is entered, a specific file location may be pulled up.

FREEDOM OF INFORMATION OFFICE

Mission and Scope. The Freedom of Information Office (FOI) is responsible for answering all FOIA and Privacy Act requests. The Consumer Product Safety Commission has only one system of records subject to the Privacy Act, so that its activities in the privacy area are much less than in FOI. The system of records is made up of accident reports, and since retrieval is not carried out by the victim's name, they are not witheld on Privacy Act grounds. The agency's policy, borne out by the regulations, is to disclose when possible.

Two sets of records fall under FOIA: regulatory and injury-related. Regulatory documents are the files that the Commissioners see, and on which they make decisions affecting the industry as a whole. These files, called decision packages, are compiled by staff members. Each pertinent staff person contributes to the package (e.g., a report from Epidemiology, one from Economics). The Office of the Secretary of CPSC compiles the packages.

The second type of record concerns product related injuries. The name of the file changes as an investigation proceeds through the agency. First it is an injury file, then an investigation file, then a compliance file, and sometimes a recall file. CPSC receives about 10,000 consumer complaints per year, which are filed by product name. These come from the consumer Hotline and written complaints. About 1,000 of these are followed up by the surveillance desk, which does an investigation report. A complaint then goes to engineering and health divisions, which investigate and test the product involved. The investigation process can also be set in motion by a petition. At about the same time the file goes to compliance and enforcement attorneys, who deal with the manufacturer.

Requests and Procedures. About 50 percent of FOI requests are for the injury file made by an attorney who has a similar case (e.g., everything on Stevenson bicycles, Model X). This includes the investigation made, if any. The victim's name is usually purged (see section on Outreach Coordination office). About 30 percent are for regulatory documents, and the rest are general information requests. Requesters of general information are often sent the regulatory documents.

The office has about 80 fact sheets available for distribution. The Outreach Coordination Office prepares the publications, and FOI sends the information out via an automated mailing list prepared by the contractors. FOI also sends out briefing packages, which are fuller than fact sheets, in response to specific requests. These cover a variety of subjects, only some of which require rulemaking. A decision package (containing the regulatory documents) may include a briefing package.

Under Section 6 of the CPSC Act, a manufacturer or private labeler, who is identifiable in information sought under FOIA, must be notified of the requested disclosure and given an opportunity to claim that the information contains trade secrets and is therefore barred from disclosure.

The statute also requires that CPSC give the manufacturer the opportunity to comment on the accuracy of the product information sought to be disclosed. While the act only states that the manufacturer must be provided a summary of the information, CPSC sends the whole file for comment. Through 1980, manufacturers were sent a printout summarizing the data. Because of complaints that the accuracy of data was impossible to assess, the Office of the General Counsel changed the FOI procedure.

FOI must pull the hard copy of an investigations file and send it to the manufacturer. The investigations file may contain photos, analyses, police reports (if any), or clippings. If the manufacturer says they do not manufacture the model in question, then the information can be witheld--a decision made by the FOI office, or, pages may be removed from the file and the purged file sent out.

About 40 percent of requests are answered in 10 days, because the office anticipates requests for briefing packages on hot topics. The 10 day time limit is often ignored, however. No one complains, since it is common knowledge that the procedures take time. Occasionally files are held up because it is known that premature notification of the manufacturer could limit the investigation.

Internal delays are caused by the following:

a) FOI deals in hard copy only

b) When the FOI office receives a request, they pass it on to the department concerned to reply. This process takes about a month.

c) There is then a Section 6 review, under which the manufacturer is allowed 30 days to respond. Ninety percent of the manufacturers request confidentiality.

d) The FOI office must then wait for a General Counsel attorney to be assigned. The attorney reviews the case, and the manufacturer may be notified again that CPSC disagrees with the claim of confidentiality. The Office of the General Counsel prepares these notification letters, which are sent out by FOI.

e) There is a second 10 day response period.

Very few manufacturers dispute the issue after this. The Director of the FOI office has only been sued 12 times, 8 of which were over confidentiality disputes.

A new system is planned which will index all compliancefiles, and all those processed by FOI, so that the clerk can locate a file and tell whether it is open or closed. Each request is entered on a Control Sheet form.

Staff Training. Every new staff person is trained by the FOI office on privacy concerns, and by the Justice Department, which gives courses on the Privacy and Freedom of Information Acts. There is a constant reminder in the FOI division, and in the agency as a whole, of the importance of the issue of privacy as it relates to manufacturers' identity and trade secrets. Privacy of accident victims is not an issue in the FOI office.

Changes Since 1980. Section 6 has created an administrative burden, and caused backlogs, because there have also been budget cuts, and less staff is available to comply with it. But the results have, in some ways, been positive: the manufacturer's name is not just "thrown around" any more. There is also more care taken with trade secret information handling. Staff is trained to recognize this information (customer lists, sales volume data, and company engineering). Trade secret information is locked up in a safe and can be sent back to the company if requested.

DIVISION OF HAZARD AND INJURY DATA SYSTEMS

Mission and Scope. This office comes under Epidemiology, which, along with Health Sciences and Engineering, is one of three technical departments which collect and

analyze data and report their findings to the Commission. Epidemiology investigates consumer accidents. Health Sciences and Engineering produce their own technical data through testing. This division of Epidemiology builds the computer file and also provides data to the National Injury Information Clearinghouse.

Computerized File Systems. The Hazard and Injury Data Systems division creates and maintains four computer files. Three are injury information data bases, called surveillance systems. The fourth is a file of followup investigations called the Indepth Investigations data base, or INDP.

The surveillance systems used are:

1. National Electronic Injury Surveillance System (NEISS). There were 250,000 NEISS cases recorded for the past fiscal year. NEISS uses a modern interactive system, with online editing capabilities. It replaces the batch processed teletype which was used until 1982.

A coder, who works for one of the reporting hospitals, uses the hospital terminal and reports cases from Emergency Room records, using a coding manual which includes CPSC criteria. Certain products and types of accident are excluded (e.g., horseback riding, bottle openers, glass, flatware) under present policy guidelines.

2. The death certificate file (DTHS), which contains certificates of product-related deaths from each state and many large cities. There were 15,000 certificates for fiscal year 1984, 7,500 of which involved products investigated by CPSC.

3. Injury and Potential Injury Incidents (IPII), whichrecorded approximately 21,000 reports for fiscal year 1984. Data comes from many different sources, such as:

a) incident reports (consumer complaints)
b) newspaper clippings
c) MEDCAP (medical examiners' reports on deaths)
d) government agencies (mainly complaints to the FDA and the National Traffic Safety Board)
e) Selections from legal publications (e.g., CAAL, Lawyer)
f) reports from Consumers Union
g) reports from ATLA (trial lawyers' association)
h) reports from selected regional fire departments (chimney fires only)
i) reports from paid MEDCAP (medical examiners paid to generate reports on interesting cases).

Investigation Procedures. A statistical sampling of all cases is chosen for detailed onsite or telephone investigation. One-third of the investigations are of NEISS

data. The NEISS file itself comes from hospitals selected as a statistical sampling. Topics for investigation are chosen by random selection within specific product areas covered by the CPSC, giving strong statistical support to the data.

If selection criteria are met, the hospital is notified of the need to identify the victim. Using the NEISS data, an Indepth Investigation Record is started, to be enlarged later. Even brief telephone investigations go into this file. The original hard copy of the investigation file is stored at the Clearinghouse for a few years, with copies going to the analysts in the technical departments. Cases are frequently sent to regional offices for investigation, such as the reenactment of an accident. A tracking file is set up, giving the status of cases.

Privacy Issues. The division is highly sensitive to privacy issues. CPSC must negotiate with hospital attorneys before a reporting hospital is chosen. There are 64 of these at present, down from 72 in operation until 1984.

Hospitals are very protective of their patients, who are listed only by number, with no identification in the records. If an in-depth investigation is required, the hospital is contacted. Some hospitals insist on contacting the individual first; most allow CPSC to do it. Until a year ago the victim's name was always purged from any output from the Investigations data base. Now they ask the victim's consent to use the name, as most are more than happy to be contacted by a manufacturer anxious to make amends. Retrieval cannot be made from any of the files by the victim's name or Social Security number.

Except for information disclosed under FOIA, data is only released to several Federal agencies. Occupational cases are passed on to the National Institute for Occupational Safety and Health (NIOSH), which pays for the data. FDA and EPA also receive Epidemiology data. Only NEISS data is released, so no privacy concerns are impacted.

Staff Training. The division tries to ensure the anonymity of individuals and manufacturers by making staff aware of the importance of privacy. There is no formalized training.

Technological Changes. Since 1982, all the data bases have employed a system which allows linking, and common queries. The department is pleased with it and does not anticipate technological changes in the near future.

A system of minicomputers and workstations with dial in/out capability is being installed, to be used primarily for word processing. Access to the data base through the workstations is also planned.

NATIONAL INJURY INFORMATION CLEARINGHOUSE

Mission and Scope. The National Injury Information Clearinghouse (NIIC) functions both as a clearinghouse and as a records room. It has access to all the data bases produced by Epidemiology and also internal tracking files. Technical information specialists perform searches of accident files only. Internal files generate reports and mailings to manufacturers, in addition to tracking. Data information clerks access the internal files only.

Privacy Issues - Staff Training. Although there is great awareness of the need for confidentiality of corporate information, and new technical information specialists are given a copy of Sec. 6(b) to read, training on the sensitivity of data is informal. Confidentiality about personal information is not an issue, since the data bases are not accessible by name or Social Security number, and many do not even contain that information. The Clearinghouse works closely with the Office of the General Counsel on privacy issues about which the staff must be informed. The directors of NIIC and the Hazard and Injury Data Systems Division cooperate in advising investigation team leaders and coders who enter data of the importance of confidentiality and accuracy at the data entry level.

Recent Changes. Up until 1979 NIIC put all files on microfilm, and sent the hard copy of investigation files to Archives, to be kept for 10 years. The accident reports were microfilmed and then destroyed. Since 1980, they have used paper copy. Office files contain records from 1979 to present. File management procedures are being revamped to accommodate these bulky files.

Formerly anyone could come in and read files. Since the 1981 amendment to the CPSC Act, there have been many administrative changes. Section 6(b) has caused some of the greatest of these, as it has become something of an administrative burden.

Investigation Procedures. Requests are first made under the Freedom of Information Act. There is a $6/hour search charge and a 10 cent/page charge over $25. Two copies of information are made (requester pays for one) and the manufacturer is notified with one. When the decision is made to release information it must be purged. Staff formerly purged the manufacturer's name, but documents are now reviewed at the second level as well. When a printout is done, the manufacturer's name can be deleted electronically from the manufacturer's field, but the name often occurs in the fact synopsis, and that must be purged manually.

Dissemination. Criteria for dissemination are based on the Freedom of Information Act, otherwise the department policy is to send out whatever they have that is pertinent. Dissemination decisions are made by whoever is responding to the request. Requesters are sent printouts or statistical summaries based on information need. If a data base search is called for, the policy is to search the current year plus the two previous years. If an earlier search is needed, it must be specifically requested.

Request Procedures. The office receives about 500 requests for information a month. One-third of these are from attorneys; the other two-thirds come from manufacturers, students, teachers, school librarians, publications librarians, media, consumers, national associations, and other Federal agencies.

Attorneys usually want product and model-specific files, but occasionally request statistics. Non-FOIA requests are usually handled with computer printouts or prepared statistical analyses. Requests will sometimes be passed on from the FOI office. If those requests are accompanied by one of the FOI office's log sheets, they will be returned to FOI to be sent out. If either office receives a request for information on a broad area, such as substantial hazards reported by companies (as required under Section 15 of the CPSCA), NIIC sends its data to the FOI office, and they will get input from the Compliance Office.

Their only publication is NEISS Data Highlights, a quarterly newsletter describing the data files and giving a summary of numbers of injuries for each product tracked. The newsletter is sent out to people asking to be placed on the mailing list.

ECONOMIC ANALYSIS

Mission and Scope. The function of the Office of Economic Analysis is to predict the effects of actions of the Commission. Issues regarding unreasonable risk are explored. Analysts look at cost changes in products, cost of medical care, and interpret and price data from Epidemiology. They examine any effect: social, economic, market changes, consumer or behavior changes, resulting from these actions. The office collects data in the form of consumer surveys, market studies, sales figures, and changes in industry costs. Staff use the publications of the Departments of Commerce and Labor, and of trade associations. They also purchase commercial studies.

Privacy Issues. This office maintains no personal data on individuals, but company identity and proprietary information are big concerns. They use CPSC internal procedures on safeguarding information. Confidential information can be sent to the Commmissioners under separate cover, rather than with the briefing packages. Trade secret information is kept in a safe. There is no confidential information in the Injury Cost Model computerized file, or in the Economic Impact Reports they publish yearly.

Requests and Procedures. The office receives one or two requests per month for cost information, according to one division director. These can be requests for printouts, requests for methodology from researchers, or for information to be used in reports and speeches. The Office of the Secretary allows the dissemination of this information, but all requests filled must be documented. Requests are sent via an internal clearance process (through a division director, an associate executive director, then to a Congressional Affairs officer if it is a Congressional request).

The other division director estimates that they receive 15-20 requests per month. Many of these can be requests from one company if the Commission has made a new rule, or if a particular topic has become a hot one. Very few requests come in for Economic Impact Reports because the Commission has not been promulgating. Types of requests received are: memos, contractors' reports, preliminary impact analyses, or final analyses (like market analyses, or potential for compliance with voluntary standards).

When Commissioners announce new findings on products, staff expect calls from the press. Each staff person answers questions, but tries to refer them to a specialist in the area concerned. The office has a staff of 15, including 2 division directors and 3 secretaries. The rest are economists.

Dissemination Criteria. The office has no formal criteria for dissemination of information, but an informal rationale has evolved based on the type of information being requested, and potential use of that information. Requests for data which are clearly public are filled without question. Cost information is an example of readily disseminated information. Requests from university-based researchers are generally honored upon request. Manufacturers requesting market analyses and product line data are screened more carefully. They will do some, however, and send some to FOI, but will tell others that they have done no work in that area.

Computerized Files. The main files used by this office are the Injury Cost Model and the CHIP (Chemical Ingredients in Products). The Model can be run with NEISS data. They use CHAMPUS for source data on injury medical costs. The Model can

be applied to this data, and to frequency and characteristics data on injuries. It produces a large picture of total costs such as lost wages, transportation, time away from home and work, and pain and suffering. Requests for the CHIP data base are usually from consumers who want to know why they got sick from Product X. A search will be conducted and a chemical staffer may reply that, for example, the product contains formaldehyde, but will not state the amount as that could be proprietary information. The data base does contain formulas. No one has ever asked for a printout, but could get one which contains disclosable information. Summary reports are usually sent out.

Future Plans. The Economic Analysis office plans to install some PCs, to be used for economic analysis using spread sheets. Some word processing support is also scheduled, which may or may not involve the PCs.

LIBRARY/INFORMATION SERVICES BRANCH

Mission and Scope. The Library/Information Services Branch provides reference service to the public, and inhouse. Anyone may access the Quick Index to library holdings (the indexed documents collection, such as research reports, not the legal collection and other holdings). This was formerly an online interactive system with terminals throughout the agency. Since the mid-1970's it has been reduced to a batch system, with research reports and technical articles being coded and indexed by Automatic Data Processing staff. All items are coded as "cleared" or "not cleared." Items not cleared must be so indexed under the FOI rules. The index contains 16,000 items.

The Library/Information Services Branch contains an extensive legal collection: reports and technical articles prepared by contractors; inhouse analyses; National Bureau of Standards reports; National Technical Information Service reports; public information publications of CPSC; and speeches by the Commissioners.

Request Procedures. Approximately half the requests are from staff—Epidemiology or FOI office personnel working on FOIA requests--and half from the public. Despite staff cuts since the 1970's, and more within the last month (the staff of 15 is now reduced to 1), the number of requests to use the Quick Index has remained the same. The office handles about 10 phone calls and 5 walk-ins a month. FOI staff come in about twice a week. Many of the public users are prospective contractors.

Future Plans. A proposal is now being prepared for contracting out all technical

services—cataloging, acquisitions, interlibrary loan, circulations, data entry into the online periodical management system, and looseleaf filing. The director will continue to handle managment and reference.

OUTREACH COORDINATION OFFICE

Mission and Scope. The Outreach Coordination office develops publications providing information to the public on the use of consumer products. A list of high visibility products is chosen by the Commission every fiscal year to be researched and written about. Ongoing seasonal projects are also prepared on subjects such as fireworks, toys, heaters, and fire prevention. Specialists obtain information from all divisions of CPSC in the form of statistics, research reports and analyses. They write up this information, and distribution is taken over by a contractor, St. Elizabeth's Hospital, to whom callers on the Hot Line are referred.

The office also produces the Spot Master, a series of short interviews and statements about products that are available on tape. This recorded information is available to the media, but not to the general public.

The Outreach Coordination office has been cut drastically since 1981, when the staff of 60 was reduced to about 4. According to a member of staff, graphics services, correspondence, more information for the media, film loans, and programs "too numerous to name," formerly provided, are no longer available. Various Outreach activities were also contracted out before 1981, but these too have been discontinued.

DATA ANALYSES AND SYNTHESES

The Consumer Product Safety Commission is not greatly involved with information technologies. The automation of agency operations, current and future, mostly increases staff satisfaction and efficiency. Of course, the general public and CPSC's specific constituencies benefit indirectly from any such improvements. The Commission's largest constituency is made up of consumers, product users, consumer groups, and those affected by the use of consumer products. Another important constituency is drawn from industry: manufacturers, distributors, private labelers and trade associations.

Eight criteria were developed in this study to assess the implications of agency practices in the three civil liberties areas of access to rulemaking, personal

and company information practices, and the provision of public information.

1. Constituencies Affected. The first criterion looks at the constituencies that are affected by agency policies and practices, especially those that employ information technologies. CPSC has computerized their information collection activities, such as the National Injury Electronic Surveillance System. Protection of consumers is enhanced by this data collection system because the agency's ability to effectively regulate the manufacturing and use of consumer products depends on reliable sources of information on which to base their investigations and conclusions.

Increased automation of the information handling procedures of the agency, such as the FOI tracking system and the online capabilities of the Hotline, benefit the consumer constituency by improving agency response time to requests for information, both under FOIA and for general information. Hotline operators will soon be able to increase the scope of information available to callers when their online search capabilities are extended to include older press releases and other information.

The basic agency policy, regardless of technology use, is to protect the information rights of both their consumer and their industry constituencies. This will be discussed in greater detail below.

No negative effects on CPSC constituencies were discovered in any of the agency information policies, practices or uses of technology.

2. Public Meetings and Comment on Proposed Rulemaking. Technology has not altered the number or type of meetings held by CPSC. The Commission has no plans to meet by video conferencing due to the expense entailed. CPSC's present procedures for informing the public about meetings go beyond the requirements of the Sunshine Act. In addition to placing notice in the Federal Register, the Office of the Secretary publishes a Public Calendar. The Public Calendar gives notice of meetings and persons attending, the topic to be discussed, and whether it is closed or open. A log of meetings is also kept available in the public Reading Room, and published in the annual report.

Comments on proposed rules are still submitted by nontechnological means, and that practice is expected to continue.

3. Dissemination of Publications. Nearly all the offices of CPSC that were researched disseminate public information in some form. The National Injury Information Clearinghouse, in addition to data sent out in response to FOIA requests, disseminates statistical and general information to the public in the form of printouts and prepared analyses. Their only publication continues to be a

quarterly statistical newsletter.

The Outreach Coordination Office, the primary publishing division of the agency, has experienced definite changes in the number and type of publications issued since 1981. The curtailment in office services and publications has been due to program changes and reductions in force. Severe cutbacks in staff have necessarily restricted the programs this office is able to provide. There have been no new technology applications.

4. Contracts for Dissemination. Contracts for dissemination of public information have also been eliminated since 1981 in the Outreach Coordination Office. The agency's principal dissemination contract still in existence is with the D.C. Association for the Retarded for the warehousing, handling and mailing of consumer information packets.

5. Library Closings. The library of the Consumer Product Safety Commission has not been closed, but its staff and budget have been severely cut. Because of funding reductions, access to the Quick Index to research reports and technical articles has been reduced from an online interactive mode throughout the agency to manual access available only through the library. Where formerly the library employed a number of staff members to clip, index and enter articles, all indexing and coding is now done by ADP staff.

Due to the extreme reduction in staff, the library is preparing to contract out all but its management and reference functions.

6. Marketing. Public information is disseminated by CPSC primarily in response to consumer requests for information. No marketing documents per se are done. The agency does however market its publications and services through press releases and conferences held by the Commissioners when they are announcing a concentration of effort in one product area. The recent campaign to make consumers aware of potential dangers in nursery products is a case in point. When a product or line of products is chosen for high visibility, fact sheets are prepared by the Outreach Coordination Office and their availability is publicized.

7. Personal and Company Information Rights. Throughout the agency there appears to be a great concern for the privacy of companies and individuals. Both computerized data bases and paper files are handled by procedures adequate to ensure privacy. The initial collection of data and the creation of data bases are done so that privacy is maintained. Freedom of Information Act requests are handled so as to assure confidentiality of accident victims, if desired, and of the manufacturer's identity and trade secrets, yet the agency policy is to disclose

information whenever possible. Technology use in the FOIA area is limited to internal tracking of files and requests, practices which increase the ability of the staff to satisfy the large number of requests for files.

No infringement of information rights was found at CPSC.

8. Security Procedures. The review of records management and computer security now in progress at CPSC will, when completed, create management procedures sufficient to ensure the security and confidentiality of personal and company information. Three information classification levels have been determined, and specific physical and ADP controls for each level of classification developed. A manual of Information Resources Management is also being written, along with a training program.

TOPICS FOR FURTHER RESEARCH

The Consumer Product Safety Commission merits another look once its ongoing automation projects are completed. At this point, it is difficult to draw conclusions on the impact of technology use based on limited agency use.

The current records management and security review, and resulting guidelines, will serve as a useful basis from which to develop future studies. In December 1984 two CPSC field offices will go online and be able to communicate with the Central Office. The implications of electronic mail use should be evaluated in areas such as security and access control, and maintenance of a signature chain. Intragency use of electronic mail should be investigated, as well as the security concerns of data access and integrity, whenever the inhouse workstations become operational for information access and communication.

Once internal tracking systems are fully operational, a small portion of a study of the above concerns might evaluate the effectiveness of such systems on agency response time and thoroughness.

4.3 DEPARTMENT OF ENERGY

INTRODUCTION

The Department of Energy was established by the Department of Energy Organization Act, approved August 4, 1977 (42 U.S.C. 7131), and effective October 1, 1977, pursuant to Executive Order 12009 of September 13, 1977.

The Department of Energy provides the framework for a comprehensive and balanced national energy plan through the coordination and administration of the energy functions of the Federal Government. DOE is responsible for long-term, high-risk research and development of energy technology; the marketing of Federal power; energy conservation; the nuclear weapons program; energy regulatory programs; and a central energy data collection and analysis program.

The Department of Energy is on the forefront in the use of information technologies, especially computerized data base management and data analysis systems. The Department utilizes a wide range of computer technologies for research and development projects, as well as for management information systems. The technology ranges from supercomputers down to the personal microcomputers implemented in office automation systems. On the whole, public access to information and rulemaking, and the dissemination of public information are still provided through traditional channels, however.

These and other issues are presented in the followingdiscussion. Due to the limited scope of this study, the focus has been primarily on department-wide civil liberty and technology activities. Only one program division is included, that of the Energy Information Administration. Organizational units are first described followed by an analysis of civil liberty implications.

REFERENCE AND INFORMATION DIVISION

Mission and Scope. The mission of this office is divided into two procedural areas. The first is to establish departmental policy on Freedom of Information (FOI). The FOI statute sets out the policy implementation for FOI as well as establishes the policy and procedures for exceptions. It has been the practice of this office to follow the letter of the law in matters of policy interpretations and determinations. Consistency is the concern in making interpretations of existing policy. Changes in policy are not implemented until legal precedents have been set to support them.

The second area of responsibility is operational. This office processes all the FOI requests for Department of Energy headquarters. When FOI requests are received, they are logged in and determinations are made as to which Program Office should take responsibility for answering the requests. Requests are then sent to the appropriate Program Office for further processing and final action. The FOI Office notifies the requester as to which Program Office is handling the request. The FOI Office monitors the Program Office responses to the requests, and maintains a follow-up system to assure that all requests are responded to within the legal time limits required. Open files constitute a great concern for the FOI Office and are closely monitored.

Closed files are maintained by the FOI Office and contain a copy of the answer to the request. The paper files are maintained by the office for up to 3 years as the statute requires. The files are then microfilmed and archived.

The FOI Office is also responsible for considerations of fee assessment and fee waivers. Denials for requested information are prepared by the Program Offices, but are submitted to the General Counsel's Office for review. All denials must be approved by the General Counsel.

The FOI Office also has the responsibility for the FOI Reading Room facility. Program Offices submit "public information" materials to this office for inclusion in the Reading Room materials.

Approximately 2,000 FOI requests are processed per year. While the major emphasis of these requests four to five years ago was on regulatory matters, there has been an increasing emphasis on nuclear waste management issues and energy research. A continuing workload has been generated for information about procurement decisions and contracts. Three types of requesters have been identified: major corporations (procurement information) and law firms (regulatory matters); special interest groups (waste management), and private individuals (research issues).

Staff training on the sensitivity and privacy of agency records is accomplished through the security clearance process. As part of this process, each person is required to attend briefings on the sensitivity of agency records and classified materials. Staff sensitivity on privacy issues is also supported by the office's policy of maintaining privacy of records.

Use of Technology. The procedural system for handling FOI requests is presently a manual system which is in the process of being automated. Operationally, the automated process will follow the same procedures as the manual system. The

automated system will, however, provide new report capabilities; for example, the system will provide the capability of generating reports by program office or by the number of open cases. Follow-up procedures will remain the same, as these are particular to each case.

Changes in the Information Practices of the Agency. From a policy point of view, there has been little change in information practices. This office maintains consistency in practices and follows the letter of the law in interpretation and determinations. Individual program office trends may have changed, and General Counsel may have detected trends in the types of denials, but this office remains consistent in its policy implementation.

There has been a major change in the types of people using FOI for discovery, with an increasing emphasis on individual research, either in matters of nuclear waste management or in energy research issues. There has also been an increasing use of FOI; people are becoming more aware of the FOI procedures and are using them more frequently. This increased use raises questions about the amount of effort required to produce the increasing amounts of information vs. the actual benefits of the information to the requester.

Impact of Information Technology on Information Practices. Because of information technology, especially automated information systems, more information is more readily available to the public. For example, numerous computerized listings are produced as reports of systems. These reports were never generated before the use of computers, but are now prepared and are available almost as a matter of routine. The law does not require an agency to create documents, but some of the previously "unavailable" information is now "created" as a matter of course because of the information system's capabilities. The public now has access to this information under FOI.

Along similar lines, information technology has also provided expanded access to information. Automated files of information provide an easier and more extensive access to information that may not have been maintained previously. The searching capabilities of systems enhance the retrieval of information in ways not previously provided by manual systems. In terms of automated systems, however, the public does not have direct access to the information system files. (In fact, at the present time, most information requested from DOE is not computerized; it is in hard-copy form. The exception is the Energy Information Administration data.)

The FOI office is caught between the "cross-fire." The Government requires that the FOI service be provided at the expense of minimum resources. This office

tries to be efficient and effective, but must still provide service. Information technology will make the reporting burden greater: more information is collected, more data files are created, and it will present greater difficulty in searching and assuring that a search is complete and exhaustive. There must be some way to provide a compromise that will reduce the reporting burden and still satisfy the request for increasing amounts of information. A solution that will benefit all parties involved must be found.

Members of the FOI Office are aware of the various ways that information technology impacts privacy activities. Of great concern are the office automation projects which utilize the off-the-shelf software packages. These are easy-to-use programs which allow the individual to set up information systems that potentially could violate the Privacy Act. There are no mechanisms to control or monitor these small, individual systems. Big systems offer greater control. While the personal computers make the job easier, policing personal computer activity is very difficult; there is no way to monitor what is being kept on the individual files. The possibilities of networking the personal computers presents even greater challenges to those responsible for Privacy Act compliance. The networking capabilities make "unauthorized" access relatively easy. The present solution to the problem is to make individuals aware of computer capabilities, make them sensitive to the problems of privacy issues, and allow the individuals to police themselves in using the small, personal computer systems.

GENERAL COUNSEL FOR GENERAL LAW

Mission and Scope. This office provides legal advice on a wide variety of areas including Privacy Act and FOI requests/denials. This is a "watchdog" function as exemptions are only asserted when there is strong legal basis.

Before a denial is made, the General Counsel reviews the denial letter and the accompanying package of information to see if the General Counsel concurs with the Program Office's decision for denial. This includes a review of the language of the letter to determine if it accurately describes reasons for denial.

Nature of Advice and Counsel. Advice and opinions are generated on both a formal and informal basis. All internal directives coming from the FOI office are reviewed by General Counsel as a matter of policy. Informally, General Counsel maintains a constant exchange with FOI staff and provides assistance as needed.

Other orders, including those dealing with technology and notices of newsystems, are reviewed for FOI and Privacy Act implications. The General Counsel tries to make people sensitive to FOI and Privacy Act concerns. This includes making program office staff sensitive to system design considerations, including making them aware that the system of records and retrieval routines comply with the Privacy Act.

Training. Within the General Counsel's office, certain attorneys specialize in the area of FOI and the Privacy Act. These attorneys are assigned the cases dealing with these matters.

Outside this office and within the agency, Privacy and FOI attorneys used to participate in agency seminars on sensitivity of data and privacy issues. These seminars have been discontinued for lack of interest.

The Assistant General Counsel is responsible for briefing political appointees and senior level employees on various acts including the FOI and Privacy Acts.

Role in Rulemaking. Advice in rulemaking is decentralized. While the General Counsel's office is not required to see every rule, it does provide advice on an informal basis. Advice can be given to individual program areas to define what the parameters are, what notice must be given, etc. Responsibility for regulatory impact and flexibility analyses lies with the individual program office. Review by General Counsel is only to make sure that these areas have been addressed. Under Executive Order 12291, The Deputy General Counsel for Legislature and Regulations serves as the focal point department-wide for review of all proposed and final rules and regulations before their submission to OMB for clearance and publication in the Federal Register.

Trends. DOE is slowly but surely entering the computer age. Presently, the impact has been manifested in better maintenance and retrieval of information without major changes in the way the information has been processed. Although there is more data available, data is continuing to be processed in a similar manner. There have been no major pushes to re-evaluate. The thrust has been to make people sensitive to the issues raised by the FOI and Privacy Acts.

One possible impact of technology may be in the different type of questions that will need to be confronted. For example, FOI requires that the requester be specific about the information requested. The courts have upheld a high threshold for the specificity of these regulations. Yet, with the increasing amount of information being collected and stored, and the different methods of retrieval and access available, this threshold may have to be redefined. As yet, neither the

General Counsel's office nor the courts have addressed this problems. It may, however, become an issue.

MANAGEMENT INFORMATION SYSTEMS, HEARINGS AND APPEALS

Mission and Scope. This office acts as an adjudicatory arm of the Department of Energy. It considers all administrative appeals and requests for exceptions or relief. These requests and appeals primarily concern corporations who find that a particular rule or order issued by the Department has caused them a serious hardship.

Appeals Process. The appeals process requires several steps. Appeals are initiated after a rule is made or an order issued. To collect evidence on the matter, evidentiary hearings are conducted to allow for public comment. Public notification of these hearings is accomplished through the Federal Register. After the hearings process is completed, the findings are analyzed, and final judgments are made on the matter. Any further appeals are taken up through Federal District Court proceedings.

This office is also responsible for the distribution of refunds that may result from a decision in a case. This refund process requires that DOE notify the general public (e.g., individual citizens, wholesalers, jobbers, etc.) that these monies are available. Notification of the distribution of these monies is also accomplished through the Federal Register. Procedures for applying for these refunds and the procedures for distribution are established by this office. Public hearings are conducted to gain public input into the decisions on the distribution procedures. Plans for distribution are finalized once the hearings process is complete.

A computerized case tracking system has been developed to maintain the petitions for appeal and to track their status from receipt through final judgment. The system has been in use for 11 years. The system is housed on the Energy Information Administration's mainframe computer, and hardware maintenance and software upgrades are provided by EIA support services (usually through contractor services). System records and record quality control are maintained by hearings and appeals office staff who are responsible for data entry and maintenance, oversight, and management review of case records. Access is restricted by password protection to only those authorized persons who are involved in the clerical functions or professional review of case records.

The case tracking system has been designed as a management tool, and theinformation collected for each record is used to facilitate the management and review of each case as it proceeds through the appeals process. The system consists of two parts: Refund Case Tracking System and the "Basic" Case Tracking System. Appeals or exceptions requests are entered into the system after they have been received by the docket/publications office and assigned a case number which identifies the category or type of request. No special form is required for making requests. Case records include the name of the company/individual making the request, case number, type of relief/request: e.g., allocation, price refund, FOI; name of attorney/supervisor assigned; status: pending, final; date received; date for analysis/review; date for review committee; proposed decision on order; final decision on order. All case records are kept online in order to facilitate the review of precedents, an important function provided by the case tracking system. A statistical analysis by type of case (appeal, exceptions, refund, motions, stays, other) is generated from the tracking system.

The case folders (paper files) are archived periodically (physical storage space is the limiting factor). They are kept in a storage room in the Forrestal Building and maintained by this office's staff.

Dissemination of Information. All decisions and orders of this agency are considered public information and are published by the Commerce Clearing House, Inc. (CCH), a private organization. Copies of final decisions are also available to interested persons through the public docket room.

This office is also responsible for processing appeals to FOI determinations (denials). These requests are processed similarly to other appeals or exception requests. Once the FOI appeal is received, it is entered into the case tracking system, and assigned to a professional for further processing. The FOI appeal procedure is outlined in the FOI guidelines.

There are no future plans for electronic dissemination of information, as this method may be to the disadvantage of those people unable to afford it. The policy for this office is to remain consumer-oriented.

Public Hearings. Inclusion of the public in the hearings process is considered very important, particularly in cases of the distribution of refunds. The hearings are evidentiary, and fact-finding. Public comment is considered necessary to the determination of cases. While requests have been made to close the public hearings, requests have always been denied.

Teleconferencing has not been considered a workable solution for conducting

public hearings. Because evidence must be presented at the regional hearings a teleconference would not provide the means for reviewing the physical evidence as presented. Also, the need for a court reporter would be compounded if teleconferencing were used.

Future Plans for Technology. The current "basic" tracking system meets the present needs of this office. There are no plans for updating the basic system or for changing its function. There are considerations for expanding the refund system. The present refund system may be made larger, or a duplicate system created with greater storage capabilities.

Attitude Toward Technology. Technology has been helpful; computer technology has expanded access. The system organization with listings of case status (receipts, pending cases, final cases) has made it easier to provide access. Personal computers have provided analytical tools (mathematical and financial calculations) as well as the case tracking functions that have been made possible by computers, providing for faster, more efficient processing of a case, analysis of the case, and projections of impact (financial).

The use of technology, however, will not alter the present mode of operation. The policy of this office has been to provide open access to information. Access will not be restricted by computers.

OFFICE OF AUTOMATIC DATA PROCESSING (ADP) MANAGEMENT

Mission and Scope. This office is responsible for developing policy, planning, budgeting, and conducting oversight reviews of the Department's computerized management information systems (MIS), unclassified security, and office automation projects. To carry out these administrative functions, the office maintains inventory systems for each of the management information systems, including a hardware inventory system that records what kinds of computer hardware are in use in DOE. Another inventory system, the Computer Utilization Information System, details computer usage and provides a status report on the number of usage hours, idle hours, and down-time.

A long-range planning report is prepared to project needs and programmatic considerations over a five-year period and is used for determining budget appropriations. The long-range plan lists program requirements, details programmatic needs, projects capacity needs and costs, and itemizes planned acquisitions. The data collected from the sites for this long-range plan is not considered public

information, but rather planning data for internal use only. The data becomes public information through FOI requests after the budget has been submitted to Congress. An Agency Composite Plan, based on site data, is available through FOI. FOI requests are filled with the framework established by the Department.

Burden Reduction. A formalized review program was instituted last year as part of a DOE management intiative for reducing the government's reporting burden. As part of this review program, a management program has been developed to quantify the burden as associated with the policy and procedures required by this office. The basic questions addressed by this review are: What use is made of the information collected and how effective is its use? The program will establish baseline levels and review various program areas to monitor ongoing efforts for burden reduction.

Training on Sensitivity of Data and Privacy Issues. Employees undergo in depth training sessions on sensitivity and privacy of data/records. Security seminars and formal education programs are presented. The great emphasis on training follows the Department's concern for security. Training has been emphasized even more so in the last two years.

Attitude Toward Technology. The implementation of microcomputers represents the single biggest impact on information practices. The office automation projects enhance the capability of people to carry out their work tasks and activities. Microcomputers permeate all aspects of the organization. Microcomputers present a security problem, however, as there is a greater capability of penetrating microcomputer systems.

Future Plans for Information Technology. DOE is clearly far ahead in the use of information technology. Long-range plans provide technology forecasts. Some laboratory sites are on the "cutting edge" of information technology research, development, and use. Supercomputers and mass storage are already being implemented, and the proliferation of microcomputers is advanced compared to that of other departments. Review of policies and practices are conducted continually to keep up with the advanced information technology use, with changes in policy and practice made as mandated by the findings of the reviews.

OFFICE OF COMPUTER SERVICES AND TELECOMMUNICATIONS MANAGEMENT

Mission and Scope. The mission of this office is to serve headquarters with computer and telecommunications services. The tasks and activities associated with this mission are accomplished by four divisions.

1. ADP and Communications Services Division is solely responsible for the procurement and operation of hardware and software. This division deals with the operation of the minicomputers and procurement of the microcomputer technology.

2. Telecommunications Divisions takes the responsibility for the telecommunications facilities and activities; most notably, the telephone, FAX, and time-sharing facilities. Other areas of responsibility include SACNET (secure network, link to field operations), radio and electronics, service on Congressional committees with interest in telecommunications, experiments with GSA on satellite communications, and IX procurement for the total rewiring of DOE facilities to expand the use of microcomputer technologies and major computer equipment.

3. Planning and Performance Assessment division provides quality control, participates in Automatic Data Processing policy development, and performs acceptance testing of major systems.

4. Information Systems Division acts as the interface between technocrats and end-users.

a. Project Management Officers define needs, conduct requirements analysis, and build major management information systems for other users. For example, PAYPERS systems for payroll/personnel and manpower systems.
Support service contracts are used for system design.
Project Management Officers serve as interface between contractor and users. Coordination is the key function.

b. Information Systems Division is also responsible for maintaining ongoing systems at headquarters. End-user can utilize hot-line service for emergency situations; otherwise, contacts PMO to handle problems with contractor.

c. Information Systems Division responds to users who want microcomputer technology. Division personnel conduct front end studies, define functional requirements, resolve compatibility issues, and provide services support.

Data Ownership and Access Issues. With consideration for theamount of outside contracting used to support DOE activities, the question of data ownership is raised. DOE contractors provide their own equipment. Any tapes/files developed by contractor belong to the Government. Contractors cannot sell tapes they might develop. FOI access is through the Government.

Exceptions to this policy are the research and development (R&D) facilities which are operated by private contractors. Patent law governs ownership and distribution. Initial contracts with private contractors spell out patent considerations. Federal procurement regulations apply in this area.

Electronic Records Management. Requests for management information systems to handle records management have been made for administrative support. A requirements study has been conducted. The concern for records management is now part of a greater office automation study. A Freedom of Information (FOI) tracking system has also been requested. Recommendations have been made to use Uniform Pending Action System for FOI tracking. This system is designed to control action logs. It is suggested that FOI requests be included as action items.

Records management is monitored on shared resource microcomputers (Molecular system). This system is password-protected; filing space is allotted. Archiving is controlled by file size; once the allotted space is used, archiving is necessary. Records management is not as easily controlled on stand-alone systems like the IBM PC. Archiving is controlled only by the amount of physical space available for storing diskettes. This was compared to manual systems where only a given amount of space is available to store paper files.

Security Issues. DOE is highly security-conscious. First level of security is the physical or facility security protection. Buildings are secured by various means: visitors monitored and escorted; fences; etc.

Computers are secured by password protection. One mainframe is dedicated solely to secure data and personnel. Signs are posted on microcomputers to indicate what type of data can be processed on that work station: sensitive unclassified, privacy data, confidential FRD or RD, confidential NSI, secret FRD or RD, secret NSI. Most workstations are restricted to one particular level of processing.

Security protection is built into software design. Contractors must devise security plan, and security officer must be assigned. Equipment is rated according to emissions standard (TEMPTEST). Some require lead shields to protect stray emission detection. Access to file is password-protected. Some are hardwired for further protection against unauthorized monitoring.

Anyone who maintains a system can get into the files. This includes files on all computers, secure and nonsecure. Contractor personnel have access based on security clearance (6 levels of clearance; e.g., Level 2 = top secret and access to restricted data such as nuclear weapon data).

Maintaining programs and systems on microcomputer technology presented a different problem. Previous policies required that administrative personnel write and maintain their own programs and systems. But that became an unrealistic expectation because many of the microcomputer software packages were not user-friendly and were difficult to document. Training was necessary. It became cheaper for Government to hire experts to build small systems and document programs for non-DP personnel to operate.

Privacy Act Issues. The Privacy Act allows only the immediate supervisor to keep information on his/her employees. If a Social Security number is collected, the person must be informed that this data has been collected.

There are two parts to the Privacy Act: 1) protect information on individuals; and 2) charge those who hold information to keep it accurate. Automation presents a problem for the SECOND part of the Privacy Act. With multiple files of data on various systems (representing different levels of supervisors), accuracy becomes a problem. Who has the correct data? When one system is updated, how does one ensure that all other systems are also updated?

Performance Evaluations. The working policy of this office is to consider collecting performance evaluation data on microcomputer files to be inappropriate. They believe that performance evaluations should only be kept in the individual's file and in the immediate supervisor's file for further reference. Requests for building systems to house this data have been made, but refused.

Electronic Mail. Electronic mail is not used extensively. The FACS (facsimile) and time-sharing services (DIAL-COMM) are used for electronic transfer. The minicomputers have a very primitive concept of mailboxes. Problems of compatibility between differing kinds of equipment have been a barrier to instituting electronic mail practices.

Electronic mail is not appropriate for classified data. However, the secure machines pass informal messages between files, and do not use electronic mail capabilities extensively.

Security Measures for Unclassified Data. Access to the main computer which houses the payroll/personnel system is controlled by access control software called ACF2 (Access Control Facility 2). The first level of security provided by this software package is the unique password and ID (identification) code assigned to each user.

A second level of security is provided through the use of rule sets that are written to limit access to files. The rules specify user access and operation; e.g,

which users can read only, read/write, execute only. The production files and system data sets are protected by rule sets to limit access and operation. Individuals can also write rule sets to protect access to their own files. Finally, each application program level can also provide its own password and rule set protection capabilities.

ACF2 monitors system usage and provides reports of instances of denied access. The Computer Center has published a user guide which details levels of access and the procedures for access. Access lists are also posted in the Computer Center to control access to computer printouts.

Security Measures for Classified Data. At the outside, user access to classified data is controlled by security clearances defined by DOE. (Clearances between government agencies are independent; i.e., one agency's clearance does not necessarily apply across another agency. Department of Energy follows FBI and OPM clearance restrictions.) DOE security clearance levels are: (1) Weapons Complex, (2) Q-Sensitive (Top Secret), (3) Q-Nonsensitive, (4) Top Secret, (5) L-Clearance, (6) Secret. These security clearances apply not only to Government personnel but to contractor personnel as well.

Classified data is also protected by ACF2 software controls. Access lists are posted for classified data. Users must also demonstrate the "need to know" when accessing upper levels of classified data.

Additional controls have been instituted for classified data. Equipment running classified data must meet TEMPEST standards for operation. TEMPEST standards have been established on electronic equipment to provide baseline emission levels which are acceptable for security-based systems. Further, classified information has been logically and physically segregated from unclassified information.

Microcomputers and Stand-Alone Systems: Security Concerns. The microcomputer and stand-alone systems present a bigger problem for security. A departmental directive places the responsibility for day-to-day security on the Program Office. Training classes on security procedures and privacy issues have been instituted for new users and offices affected by office automation. The classes discuss "Facts Every DOE ADP User Should Know About the Privacy Act of 1974." (See Attachment 3.)

The personal computers were not developed with security measures in mind. They are not presently capable of supporting high level security packages. Some studies have assessed available security software packages, but none seem completely adequate. Some do provide password and encryption capabilities.

Information Technology Impact. Computers have greatly improved access for people who need access to conduct their jobs. Everyone now has computer capabilities to manipulate and retrieve data. However, the security features built into the system make it more restrictive. Access is limited by the security measures implemented to protect the data.

Security is really dependent on people not giving away the security controls. If staff are careless or negligent in protecting their passwords, ID codes, or rule sets, the system (or file) is threatened by unauthorized access. The weakest link in the security system is the staff member who may reveal security measures.

EXECUTIVE SECRETARIAT

Mission and Scope. This office handles the documents for the three Principal's offices: Secretary, Deputy Secretary, and Undersecretary. As the central depository for these Principal's offices, this office processes many kinds of correspondence and documents addressed to the Principals, including Congressional correspondence, public mail, and Freedom of Information requests which have been routed to this office by the FOI office. When a correspondence item is received by the office, a correspondence analyst determines whether one of the Principal's offices or a Program Office should make the reply. The correspondence is then routed to the appropriate office for further processing and action.

Use of Technology. An automated tracking system is being used to monitor the correspondence coming into and being routed out of the office. The tracking system resides on a HP 3000 computer and has been in operation for four years. Hardware and software maintenance is performed by an outside contractor; record content and quality control is maintained by this office's staff.

Access to files is controlled by password protection written into the program software. Checks for security and unauthorized use are accomplished by periodic studies conducted unannounced for waste, fraud, and abuse.

Internal management reports are generated by the tracking system. Most of these are status reports which help the Director identify pending and overdue correspondence based on the due date assigned at the time of receipt. Every Monday, a report is generated which lists the correspondence assigned in the previous week. This report is sent to all action offices and returned on the following Friday with annotations of the action taken during the week. The data base is updated on Friday after the printouts are returned from the action offices.

On a weekly basis, a high priority mail report is generated which lists the status of correspondence from the White House and Congressional Chairmen. On a daily basis, a status report is produced for all the mail sent to the Principal's offices. On request, reports can be produced which list correspondence by type of correspondence (public, Congressional, state officials, etc.), type of requester, or subject area.

Files remain open until a response is made. Action copies go the Program Office for response, with file copies maintained until the response is made. Active files contain current year plus the past two years' material. Paper files are archived once a year and categorized by source code: Congress, Public mail, state office, federal office, White House, etc. Access to files considered "public information" are made available through the Reading Room facility maintained by the FOI Office.

The automated files have only been archived twice. The archiving process was scheduled a month in advance, with certain time frames and kinds of correspondence targeted for storage. The tapes were stored in the building, outside the computer room.

Training on Sensitivity and Privacy of Records. Staff receive privacy and sensitivity training upon orientation. They also undergo continuing training courses on a quarterly basis (refresher course). Two types of analysts are employed in this office: incoming mail analyst who analyzes mail to determine to which action offices the request should be sent; and suspense analyst who maintains the data base on a daily basis, closes out files, and prepares reports.

Attitude Toward Technology. Computer technology has enhanced the process greatly. It has helped the Office to be more responsive and current. Reports generated from the tracking system assist in identifying overdue mail, determining trends in the types of mail/correspondence received, and displaying (graphics package) status and statistical measures of action/reponse by Program Office.

In conjunction with proper program management, the computer has facilitated meeting the increased workload despite the reduction in staffing. This office has absorbed 13 more program functions, with a staff reduction of 20 percent. Also, a dramatic reduction in overtime work can be directly attributed to the use of the computer.

Future Plans for Technology. Future plans call for upgrading the present tracking system for greater storage capacity. Plans also call for adding a tracking system for Congressional reports.

HISTORY DIVISION/ARCHIVES

Mission and Scope. The mission of this office is threefold: (1) to write agency's history, (2) to maintain historical archives, and (3) to provide the agency with an institutional memory. The office preserves and maintains the top agency records of the Secretary and Principals.

Requests for information do not usually come through the FOI channels but through direct request by letter or phone. Often, individuals will come directly to the office to do research. These researchers are asked to complete a form which denotes the nature of their research and indicates levels of security clearance, if any. Following the National Archives policy statement, the identity of each researcher is protected.

Over the past six months, there were 222 requests (written and otherwise) for information: 126 from offices within the Department of Energy, 30 from the general public, 27 from scholars, 21 from other Federal agencies, 9 from FOI requests, 9 from Congress, and other miscellaneous requests from law firms and the media.

Records follow the disposition schedule set up by the records management office (Office of Administrative Services), and records schedules are reviewed according to Form 35 (National Archives). As a matter of routine, all schedules are reviewed for potential historical significance. Storage space is a concern, however, as this office alone stores 3,000 cubic feet of records for only 3 percent of material which is actually kept.

Access. Access is governed by the policy that every researcher—private or government personnel—gets access equally, except for "Need to Know" requests, which receive special attention. Unclassified data is open to access, whereas access to classified data, including national security information and restricted data, is restricted to those individuals who have security clearances.

Publications are generated by this office and by request from other sources, including other government agencies. Recent publications include a history of the various agencies leading up to the formation of the Department of Energy, a study of civilian nuclear power policy, and a review of the Three Mile Island events. These publications are distributed through the Government Printing Office or through contract with commerical publishers.

Use of Information Technology. This office produces an automated bibliography of

all publications pertinent to the history of the Department. The information request activity is also computerized. This system is used as an in-house management tool which provides tabulations on request activity on a monthly basis.

Future Plans for Technology. Presently, there are plans to update the word processing capabilities of this office. There are no plans at this time for automating the records management. The biggest problem is how to archive automated records. Automating records requires enormous expense for indexing the data. Sampling techniques may be used.

Trends in Information Practices. Since the communications revolution, government has become more accountable—it must document its activities. This generates more records and contributes to paper workload. In the midst of the technological revolution more paper than ever is being spewed out. The issues of quantity vs. quality come to the foreground. The vast multiplication of word processors also contributes to this problem and will impact on record keeping. The impact has not been defined as yet, however. From a historical point of view, this multiplication of recordkeeping means there is more evidence to wade through than ever before.

OFFICE OF SCIENTIFIC AND TECHNICAL INFORMATION

Mission and Scope. The Technical Information Center (TIC) is responsible for the Department's technical information program. As an internal management organization, the Center is intended to serve the information needs of the members of the scientific community, either government or private, who are actively engaged in the expenditure of DOE funds. The TIC provides a central facility for the reporting of information generated from DOE-sponsored research. In addition, the Center collects and makes available references to worldwide energy literature and research reports and produces energy data bases and publications. To accomplish this broad coverage, specialized document exchange programs have been established with foreign countries or organizations which provide the necessary channels for the exchange of technical information reports between the United States and selected countries. In order to handle all these types of information, the Center has established a multilevel system to process classified, limited/sensitive, and unclassified information.

Access. Access to information collected by the Center is provided through online services and hard copy and microfiche distribution. Technical reports generated by DOE-funded research are sent to the Center for processing and permanent access

and storage. Approximately 125 reports are received each day. Each report is checked to determine distribution limitations, then abstracted and indexed for entry into the online information retrieval system operated by the Center. The system called DOE/RECON (REmote CONsole) was developed to provide rapid and easy access to energy-related data bases. Access to the retrieval system is made available internally to government scientists and private contractors with DOE-related research projects. Public access is made available through the DIALOG Information Services, Inc., a commercial data base vendor. Magnetic tapes of the data base are also available through the National Technical Information Service (NTIS). The system is operated on a cost-recovery basis.

Classified reports are processed into a Classified Data Base and access is limited to those with the authorized use. A Limited Reports data base contains reports with sensitive material such as proprietary or patentable information. The access to this data base is also limited to qualified users. Reports having no distribution limitations are processed into the Energy Data Base and are announced in Energy Research Abstracts and other abstract journals. These reports are available through DOE or contractors approved by the appropriate program manager. NTIS and the Government Printing Office provide the primary access for hard copy documents for public access.

The Center also maintains a file of descriptions of DOE research projects. This file is used to produce the Research in Progress file available on the DOE/RECON system. Another file maintained on DOE/RECON contains descriptions of computer software packages prepared by DOE and its contractors. The software is collected, analyzed, tested, and made available by the National Energy Software Centers operated by the Argonne National Laboratory. This is maintained through a subscription basis, and operated on a cost-recovery basis for use of the software.

The Center maintains a registry of all public information documents produced by DOE and its contractors. This automated control system tracks documents from printing through shipment to a requester.

Procurement contracts control unauthorized access, distribution, use, and computer security of data bases managed by contractors, who must sign forms that pledge that they will not provide access for unauthorized purposes.

FOIA Requests. FOIA requests are channeled through the FOI Office to the Technical Information Center. FOIA requests are handled according to the procedures set up by the FOI guidelines and the FOI Office.

Changes in Information Practices. Changes in information practices have followed

the changes in the organizational structure and function of the Department of Energy. Under the Atomic Energy Commission (AEC), access was greatly limited, as most information was considered classified. When the AEC became the Energy Research and Development Administration (ERDA), the scope of activities widened to include a whole new realm of information that had to be made available. Access was greatly enhanced. The Atomic Energy Act required by law that information should be disseminated free. Cost was not questioned.

In the last 10 years, the emphasis has been on not only educating the scientific community but making information available to the public to educate them on energy affairs. However, with computer and electronic storage and retrieval capabilities, greater amounts of information are available for dissemination. Since the 1980 Paperwork Reduction Act, questions have been raised about whether "more" is better. There has been an effort made to reduce the burden on government to publish and print large amounts of information. As a means of reducing the reporting burden, certain information centers and sources have been targeted for the specific purpose of educating the public.

Future Plans for Information Technology Use. A computer networking project has been proposed that would allow researchers from selected agencies to share resources. The proposed agencies involved in the project are NASA, Department of Defense, Department of Energy, and Commerce (NTIS). The project is now approaching the demonstration phase and will provide a means for capitalizing on research and development funds across agencies by linking information/data between research sites and allowing researchers from the various agencies access to the experimental data.

A second proposed project is to provide full-text search capabilities for the Energy Data Base. The project would involve the use of OCR (Optical Character Readers) and laser printers to process the data. Presently, this project is still under consideration.

ENERGY INFORMATION ADMINISTRATION

Mission and Scope. The Energy Information Administration (EIA) is responsible for collecting, processing, and publishing data in the areas of energy resource reserves, energy production, demand, consumption, distribution, and technology. The data that EIA collects serves two different but related purposes. First, the EIA collects data required for analyses of energy issues and for the formulation of energy policy.

Aggregate data are generally sufficient for these purposes, and access to individually identifiable data is usually not required. Statistical sampling techniques are used to collect this data. Second, the EIA collects data required for regulation and other specific program uses, such as contingency planning. Data for these purposes are usually collected on a comprehensive, company-by-company basis.

Specifically, the EIA conducts analyses on complex, long-term energy trends and the microeconomic and macroeconomic impacts of energy trends on regional and industrial sectors. Special purposes analyses are prepared involving competition within the energy industries, the capital/financial structure of energy companies, and interfuel substitution. Statistical analyses and forecasting models are used to predict the impact of various trends on the energy industry.

The EIA has developed a highly sophisticated computer system for data storage, retrieval, and analysis. This system provides for data base management, modeling, simulation, and statistical processing; text editing, table processing, and graphics packages. The results of EIA's statistical and analytical activities are published in periodicals and special one-time reports. The periodicals are grouped into families based on fuel types and appear weekly, monthly, quarterly, and annually.

Periodically, a Professional Audit Review Team (PART) reviews EIA's operations, and prepares an annual report on EIA activities. These independent onsite auditors conduct reviews to ensure the validity of regulatory and other energy data. The PART reviews are available to the public and to EIA.

Access. The EIA provides data publication and distribution services within DOE, throughout the Government, and for the public. It is a clearinghouse for general information on energy. Major users of EIA publications are Congress, private industry, state officials, and universities. Publications are sold through the Government Printing Office, and the National Energy Information Center. Several data tapes are available for the Nation Technical Information Service (NTIS), but public access to EIA data bases is strictly controlled. The EIA does provide electronic access to a read-only file of summary information released on a daily basis.

Contractors who maintain the computer system are barred by procurement contractors from unauthorized disclosure of information. Standard data access clauses are included in the contracts to protect the use of the data. Security clearances are required of government employees and contractors who have access to the data. Random checks are conducted on the data base system to uncover any

unauthorized use or access.

FOI requests are handled according to DOE procedures. The FOI office forwards appropriate requests to EIA, and an analysis is conducted to determine if the data is confidential. If not, data is released. Often, summary tables on file are suggested to the requester for use.

Public Hearings. Public hearings are conducted to allow for public input on the collection of proprietary information. The hearings are announced in the Federal Register. There is a hearings process for each survey conducted. The hearings are used to determine whether data will be collected and whether information is to be kept confidential.

Disclosure of Confidential Information. Of great concern to EIA is the disclosure of confidential, proprietary information to other DOE components and other Government agencies. Under the Department of Energy Organization Act (DOEOA), EIA is required to share information, upon request, with other components of the DOE, including the Federal Energy Regulatory Commission (FERC). This requirement means that any data collected or maintained by the EIA, including data collected on a sample basis, must be provided on a company-specific basis to all other entities within the DOE, including those with regulatory functions. EIA feels very strongly about protecting the confidentiality of the data and where possible releases only aggregate statistics. However, there are some instances where aggregate statistics are not sufficient, including the data used in comparisons for checking reporting accuracy, and analysing market behavior in specific, localized areas. In these cases, EIA cannot protect the confidentiality of its data.

The disclosure requirements to which the EIA is subject cause difficulties for the survey collection process. Companies are reluctant to provide information and are slow to respond to data questionnaires. Other agencies are reluctant to share lists of potential survey respondents because EIA cannot protect the confidentiality of its data.

To remedy this situation, EIA has imposed conditions for access to its data through the implementation of the "DOE Policy on Disclosure of Individually Identifiable Energy Information in the Possession of the EIA" (45 Fed. Reg., 59812). However, this policy does not provide adequate protection for statistical information. As a further measure, EIA has submitted a legislative proposal, "EIA Reports Reduction Act," to Congress in April 1983, that would designate certain information collected by EIA as statistical and protect it from non-statistical uses. A new proposal, the "EIA Amendments," dealing with confidentiality, is in

preparation. The document, "Progress Report: Development of EIA Confidentiality Legislation," details these legislative proposals (see Attachment 3).

Trends in Information Practices. Clearly, technology has impacted on the manipulation, processing, and use of data. It has provided more efficient processing of activities; more work is accomplished with half the people. The mission of the EIA has increased and the computer capabilities have provided better handling and processing of the data.

DATA ANALYSIS AND SYNTHESIS

The mission of the Department of Energy is to provide the framework for a comprehensive national energy plan through the coordination and administration of various energy functions, including energy research and development projects, regulatory programs, and a central data collection and analysis program. To carry out these responsibilities, DOE is heavily involved in the use of information technologies, especially computer and telecommunications systems.

Several criteria were developed in this study to assess the implications and impact of the use of information technology on agency practices in three areas of civil liberties. These three areas were access to rulemaking, provision of public information, and personal and corporate information practices. The following presents a discussion of these criteria as they relate to the information practices of DOE.

1. **Constituencies Affected.** The first criterion concerns the constituencies that are affected by agency policies and practices, especially those involving the use of information technology. DOE serves a wide range of constituencies. DOE officials respond to requests from the White House and Congress on energy-related legislative and regulatory matters; provide private industry and the public with information on such issues as energy production, reserves, consumption, and distribution; and supply scientists and researchers with up-to-date information on energy research and development.

All these constituencies have benefited from the increased use of information technologies. Computerized data collection procedures provide DOE agencies with greater capacities to store information. Access to that data is enhanced with the more powerful automated retrieval techniques available on the computerized data base management systems. The computerized statistical and mathematical manipulation of this data is far superior to manual techniques. With these enhanced

capabilities on computer systems, such agencies as EIA and TIC can ensure data reliability and validity, and provide greater data analysis for researchers, scientists, private industry, and the public.

Automated data handling and processing techniques also benefit DOE constituencies. Several computerized tracking systems are in place; these provide quicker response to requests. The Office of the Executive Secretariat, the Office of Hearings and Appeals, and the FOI office (soon to be automated) can monitor requests and cases more closely, and improve agency response time for providing information.

It remains, however, the policy and practice of the Department to provide open access to public information, and to protect personal and/or corporate information from unauthorized disclosure. The use of technology will not alter the present mode of operation.

2. Public Meetings and Comment on Proposed Rulemaking. Technology has not altered the number or type of public meetings held by DOE. Little attention has been given to the use of teleconferencing as a means of facilitating the hearings process. In the case of the Office of Hearings and Appeals, teleconferencing is not an option because these hearings are evidentiary and require the submission of physical evidence for examination. Notice of hearings is still accomplished through the Federal Register, and public comments continue to be submitted through conventional means. That practice is expected to continue.

3. Dissemination of Publications. Publications are distributed through a variety of means including the Government Printing Office, National Technical Information Service, National Energy Information Center, and commercial vendors. For example, the Office of Hearings and Appeals allows all decisions and orders to be published by the Commerce Clearing House, Inc., a private organization.

Data tapes of selected EIA and DOE/RECON system files are available through NTIS. There is no provision for direct public access to the data bases maintained by EIA or DOE/RECON. EIA does, however, provide "electronic" access to a specialized file established to release summary data on a daily basis. This data is also published in hard-copy form.

4. Personal and Corporate Information Rights. Throughout the agency, there appears to be great concern over the privacy of individuals and corporations. Agency policies and personnel training support the protection and confidentiality of personal and corporate data. Both computerized data bases and paper files are protected from unauthorized access. FOIA requests follow the letter of the law on

disclosure.

However, the EIA has identified one major problem in protecting the confidentiality of data collected for their statistical purposes. Under the DOE Organization Act, EIA must share data with other DOE components, including the Federal Energy Regulatory Commission. Under certain requests, company-specific information must be disclosed. In these instances, EIA cannot protect the confidentiality of the data. EIA is promoting legislative proposals to remedy this situation.

The policies and practices of DOE support the protection of the confidentiality of personal and/or corporate information. The use of technology did not appear to cause any infringement of this right. The only problem in this area seems to be a result of legislative mandate.

5. Security Procedures. DOE is highly security conscious. There are several levels of security in place. First, there is restricted access to the physical buildings. Second, security clearances are required for personnel, both government and private, who work with sensitive and restricted data. Third, security protection is built into computer systems design. At the minimal level, there is password identification code protection. At a higher level, rule sets built into the software programs limit access to file. Further, computer equipment must meet certain standard (TEMPEST standards) which define acceptable levels of emission. Systems are also closely monitored, and audits conducted unannounced to detect unauthorized use.

The use of microcomputers and stand-alone systems presents a bigger problem for security. Presently, microcomputers are not capable of supporting high-level security packages. The use of microcomputers in remote or isolated areas also presents a problem to security. Presently, signs are posted to indicate the level of data being processed. Further study is needed to overcome the problems of security for microcomputer use.

TOPICS FOR FURTHER RESEARCH

This study of DOE information policies and practices as they relate to information technology use and its impact in civil liberties has generated several topics and issues for further research. These issues represent concerns raised by DOE officials and program personnel and recommendations which resulted from analyzing the data for this study.

The greatest area of interest for future research is the use of microcomputer technology. All DOE program personnel noted the great promise of personal computers in extending the individual's access to information and in enhancing the individual's ability to conduct his/her work tasks. However, several concerns were raised as to its use.

o The whole problem of security surrounding the use of microcomputers and stand-alone systems (including networks of personal computers) is an important area for future research. Specifically, further study is necessary to design and develop more powerful software security packages and to test existing packages. Further, research should be directed to resolving the problems of "physical" security on systems used in "remote" or "isolated" stations. Future study could also be undertaken to develop management procedures to deal with the problem of security in the use of microcomputer systems.

o Protecting the privacy of individual/corporate information on microcomputer and stand-alone systems is another area in need of further study. Research could be directed toward developing methods and procedures for making users aware of privacy concerns and for the need to "police" themselves in establishing systems which may violate privacy concerns.

o Another issue in the use of personal computers involves the problems of data maintenance. As small systems proliferate, the chance for duplicity of data is greater. Future research is recommended to address the need to ensure that the accuracy and validity of this data (in multiple files) be maintained.

Another issue for future research involves the concerns for burden reduction. Computer technology provides the capabilities for generating more information. More data is stored; more reports/analyses are prepared than ever before. On the other hand, computer technology also provides a more efficient means for retrieving and producing data. Future research should address the "marriage" of these capabilities to facilitate a more efficient reduction in the reporting burden.

One final issue to be addressed by future research is the possible dissemination of information and publications "electronically;" i.e., providing for online access to public information via computer and telecommunications. One specific example would be to allow requesters to access automated files of public information directly. The concern here is to make "public information," not confidential information, available online. "Electronic" dissemination would open up another channel for distribution of publication information.

4.4. INTERNAL REVENUE SERVICE (IRS), DEPARTMENT OF THE TREASURY

The Office of the Commissioner of Internal Revenue was established by an act of Congress on July 1, 1982, and is responsible for administering and enforcing the internal revenue laws and related statutes, except those relating to alcohol, tobacco, firearms, and explosives. The IRS mission is to encourage and achieve the highest possible degree of voluntary compliance with the tax laws and regulations and to conduct itself so as to warrant the highest degree of public confidence in the integrity and efficiency of the Service.

Information services and information management are integral to basic IRS activities: ensuring resolution of taxpayer complaints; providing taxpayer service and education; determination, assessment, and collection of internal revenue taxes; determination of pension plan qualifications and exempt organization status; and preparation and issuance of rulings and regulations to supplement the provision of the IR Code. The source of most revenues collected is the individual income tax and the social insurance and retirement taxes, with other major sources being the corporation income, excise, estate, and gift taxes.

IRS organization is designed for maximum decentralization, consistent with the need for uniform interpretation of the tax laws and efficient utilization of resources. There are three organizational levels: the National Office, the Regional Offices, and the District Offices and Service Centers. The profile which follows was drawn from group interviews with staff at the national level.

POLICY AND MANAGEMENT

Support and Services. Divisions under the Assistant Commissioner for Support and Services include: Facilities Management, Centralized Services, Disclosure and Security, National Office Resources Management, Tax Forms and Publications, and the Data Center.

Electronic Mail. With respect to electronic mail, IRS officials describe their systems as localized and fragmented. Many different network systems are used at the national, regional and district offices. There is no overall system. There is a system called SAM ("send a message"), which accepts voice and data, and is used primarily for informal messaging. Taxpayer information sent on this system is not to be left on SAM, but it is the recipient's choice as to what to do with that data once it is on the machine.

Securities Division formulates policies for physical, data, and communications security at all levels of IRS, and disseminates these policies in a manual, which is updated as needed. The incentive for security maintenance is high at IRS because improper disclosure is punishable by 5 years' imprisonment.

Training and Security. While there is no specific data security training at IRS, new employees are given security training during their orientation to IRS and whenever they change positions. In addition, each manager is responsible for training staff about information handled in their specific jobs. Periodic updating sessions are provided. IRS produces films and has a substantial training program.

The Integrated Data Retrieval System (IDRS), which houses individual tax data, has front-end access security built into the system. IDRS can be accessed by the 10 regional centers. There are no IDRS terminals in Headquarters.

Electronic Record Keeping and Filing. Electronic systems hinder records management. IRS is not receiving adequate guidance and standards from responsible agencies. They are developing record control schedules appropriate to computerized systems anyway.

There has been a long-standing and ongoing debate with the National Archives and Records Service over which Title of the Code takes precedence: Title 26, IRS' establishing legislation, or Title 44, which sets archiving requirements for Federal records. IRS has refused to archive certain information on taxpayers to maintain data protection.

Research Division is involved in pilot projects for the electronic filing of tax returns and is discussing standards for filing with big accounting firms. IRS is sensitive to unfair competition to preparers and continues to discuss issues with the public. They are also researching home filing of individual returns.

The Criminal Division is concerned that if a person files electronically and makes a mistake of a criminal nature, it would be hard to pin down that person without a signature. IRS is also proposing a "return free" system to cover 2/3 of the filers (not the 1/3 with itemized deductions). Another test being developed involves the use of the optical disk to archive the first two quarters of 941s (quarterly employee forms) and a selected sample of 1040s. The optical disk raises issues about the legal admissibility in a court of law of reproductions from the optical disk image. These projects are all in a research phase and it is too soon to predict which technologies will ultimately prove most effective for the different IRS functions in question.

FOIA Dissemination. IRS receives relatively few requests under FOIA. Responding

to these requests is mostly a question of information content, not media. Admittedly, it is difficult and different to identify a machine-readable record as part of an FOIA request.

Disclosure. Disclosure and interpretations are the responsibility of the Disclosure and Security Division. The major policies are found in Section 6103 of the Tax Reform Act. IRS leans heavily toward the data protection side of disclosure issues. Each field and regional office has a representative of this Division of a GS 12 or 13 status. A Privacy Act request would go through this chain. There is a Disclosure Officer Training Program consisting of two weeks of intensive training, with continual updates. The Division has its own review program to oversee field offices.

Use of Identifiers. No individual dossier or profile is kept on an individual. Information is stored under IRS functions in a decentralized system. Indexing occurs in the following: Master File (accounting file), indexed by SSN; Information Retrieval File, SSN; NARS file, DLN (district location number).

IRS conducts matching mostly to identify and correct nonfiling. They have used matching of mailing lists of households to detect people who do not file at all. They also obtain information on interests and dividends from banks to detect self-employed people who do not file. Highway use tax data is also used in matching to determine whether owners of vehicles with x many axles owe returns. Outside agencies can access IRS data through the Disclosure Office, providing their request is substantiated through a legislative or other equally significant requirement.

Information Dissemination. IRS Officials report few cuts in printing and publishing, as compared to other agencies. IRS publications have traditionally been subject to strict justification and clearance procedures. When the OMB moratorium was issued in 1981, there were few luxuries in the printing budget; hence, few budget cuts. Another reason for the few changes in IRS printing and publications is due to the fact that their publications are integral to their overall mission, and are viewed as significant by internal administrators, as well by Congressional and Executive branch officials.

Publication #17 provides instructional materials on how to prepare tax returns. It is a free publication. They publish a series of smaller publications on specialized subjects, which are available on request and are also free. They publish: documents to teach about taxes; statistics of income; their annual report; and the IRBulletin. IRS Publications Services is currently experimenting with electronic

publishing by making its most used publications available online through commericial vendors. An electronic file of about 66 publications was made available on Compuserve and BRS starting February 1984. A much smaller file was put up by VUTRON (division of Knight Ridder). Statistics from February to May 1984 on Compuserve show 6083 access for 780 hours of online time. IRS officials contend that it is too soon to determine the meaning of this data as an indicator of accessibility to information or of change in constituency composition. IRS plans to continue this pilot and turn it into official practice.

Research results are generally available through FOIA. In the last year, they are making results on tax administration research available to the academic community to stimulate interest in this area.

A Teletax System makes taxpayer information available on tape to telephoners 7 days a week. During tax season, IRS staff write articles for the press and disseminate them free of charge.

The Research Division uses contractors for surveys or data compilation and for dissemination.

OPERATIONS

The Associate Commissioner for Operations includes Criminal Investigation, Examination, Collection, and Employee Plans and Exempt Organizations.

Examination. An effort is underway to automate the examination function. Computers are being used to write reports, and a pilot in Boston with 15 agents involves the use of portable computers. These computers are being used as calculators without data bases to file information on taxpayers.

Internal matching occurs in the use of the Discriminate Function (DIF) System. A random sample of returns is generated and studied for ranges of reponses on every line item. Scores to discriminate returns are developed and then each return is run through the DIF formula to determine those returns that might warrant examination. This is part of the Taxpayer Compliance Measurement Program. TCMP is a random sample program that produces data for DIF formulas. The DIF score is a probability of error and it changes every 3 to 4 years. It is run at Martinsburg, West Virginia.

Exchanges with other agencies are done ad hoc and by working agreement, such as with Customs, DEA. Data exchanges are often done with treaty partners (30+ countries). Results are transmitted by mail, and is primarily a manual process.

Tax evasion has become an international issue. IRS works heavily with Canada.

There is an Examination Branch in every Service Center. They classify returns; correspond with taxpayers; examine returns by doing correspondence audit; close out documents; and schedule examinations electronically.

Information Returning Program (IRP) involves employer sending 1099s to IRS on interest earned, which is put with W2 to create files in IRP. They run IRP next to the Master File to see if earnings were reported. They will soon have OCR equipment to read 1099s into the computer.

Collection. Security is important in this division and there is heavy training on security/privacy aspects of Section 6103 of the Code. Employees are aware of requirements and of consequences of disclosure. Training manuals written for the collection function will eventually be distributed electronically, rather than printed. There is also an IRM manual on security published at the national level.

An automated collection system has been developed which has lists of nonfilers online and a software program to dial persons, if IRS has their numbers. Four letters are sent to nonfilers. If no response is made to the collection site, a personal contact is made.

The Division has institute DEC's All-in-One office automation package, which serves as a network and allows messages to be sent to the regions.

Criminal Investigation. Electronic mail is in the planning stage, to be used for message switching, memos and mail. They are concerned with security/privacy.

Their general policy is to maintain hard copy of records and to keep records on the CPU for a short time as a temporary hold file.

In terms of computer security, legal and privacy aspects must comply with national guidelines and the electronic library of computer applications. Districts have ADP committees to deal with requests for applications, costs, security, access, maintenance, etc. Regional committees also look at computer use.

With respect to matching or exchanges, IRS receives more than it gives. In a grand jury context, there is usually a free flow of information, because no one else has access during this time.

Exchanges with DEA are usually on a query basis, not involving disclosure.

IRS can access the Customs (bank secrecy act documents).

IRS has developed a Treasury Enforcement communications System (TECS) listing tax fugitives.

Employee Plans and Exempt Organizations. As legislation is passed on pension plans, it goes to this Division for analysis, development and approval. They also

handle exemption questions, which is done at the district level. Exemptions become public record.

DATA PROCESSING

The Office of the Associate Commissioner for Data Processing is divided into two units headed by Assistant Commissioners: 1) Computer Services, and 2) Returns and Information Processing. The three divisions of Computer Services are Hardware, Software and Management Systems. Returns and Information Processing has four divisions: Returns Processing and Accounting, the National Computer Center, Statistics of Income, and Taxpayer Service.

Information Flow of Returns Processing. At the ten IRS Service Centers, money accompanying returns is accounted for. Information on the returns needed for the master file is coded. The only data from returns currently kept electronically is accounting and entity information. The coded information is validated for consistency (no name changes since last filing; no single persons filing joint returns) and mathematical correctness and then posted to the master file. Output from the Service Centers is on magnetic tape, which is sent to the National Computer Center at Martinsburg, West Virginia, for batch processing and updating on the UNIVAC.

The Integrated Data Retrieval System is created and maintained at the Service Centers. This system contains accounts (about 10 percent of all returns) on which taxpayer letters have been sent out indicating possible problems with a return. The IDRS is updated daily with Service Center information, and weekly with information from Martinsburg. All Service Center terminals connect with the UNIVAC. Microcomputers in use do not currently interface but integration of the systems is being investigated. The primary concerns in any integration project are security and response time—too much traffic on an integrated system decreases response time.

Although the ADP system has become quite complex, with supplemental subsystems, the file structure is still based on the concept of unit ledger cards.

Security. Security procedures are in place for use of connections between dumb terminals and mainframes. District Offices can access only the data bases of their respective Service Centers. Terminals within a Service Center cannot access data bases maintained at other Service Centers.

Real time systems employ passwords. Each user has his own profile of

permitted activities. The computer will terminate the transaction if activities not listed in the profile are attempted. Audit trails are built in to identify accounts worked on by each individual. Audit files, from which any information can be extracted, are maintained on tape at the Service Center. Security reviews take place the day after an unauthorized transaction is attempted.

Batch systems do not have the same security procedures. Authorization must be obtained for access to tapes. Activities are logged but there is no automatic audit trail.

Microcomputer security considerations are being evaluated and have been the subject of recent internal documents. "Microcomputer Security: A Management Responsibility" was recently distributed to managers at IRS. The three categories of microcomputer assets identified as requiring protection are software and data; hardware; and computer time. Four broad objectives are cited: 1) protect the integrity, confidentiality and accuracy of data, particularly information protected under the Privacy Act and 26 U.S.C. 6103, the IRS confidentiality and disclosure statute; 2) protect organizational assets; 3) ensure survivability of systems and assets; and 4) protect employees from temptation, subversion or threats. A security assessment checklist is attached to the document.

NEW AND PROPOSED AUTOMATED SYSTEMS

Automated Collection System. The Automated Collection System or ACS is now operational in 21 call sites. All District Offices are covered by ACS. Call sites are set up to communicate with taxpayers who have delinquent accounts and initiate repayment schedules. Case information is pulled up automatically by ACS in order of monetary priority. The computer dials the taxpayer's telephone number--unanswered calls are automatically rescheduled for a different time. The collection representative communicates with the taxpayer when contact is made and enters action taken into the system. Letters or forms needed are automatically generated by ACS. A built-in Management Information System provides checks on the system and on the representative.

IDRS data is accessed in the call sites but there is no direct linkage between the ACS and IDRS systems. ACS has the same security systems discussed above. There have been no studies done on effects, if any, of the use of ACS on the amount of discretion exercised by collection representatives. The statement was made that discretion accorded to representatives tends to ebb and flow with policy

changes.

Automated Examination System. The Automated Examination System (AES) is expected to be operational by 1987. AES will allow auditors in the field to use portable computers for audit assistance in many ways. Besides applications programs such as spread sheets, word processing and time keeping, AES will provide a rule-based expert system which will generate questions for investigation. Through AES the auditors will have access to account information and a reference system.

Pilot programs in Boston, MA and Austin, TX involving lap computers are solely local initiatives and not connected with this project.

Tax System Redesign Project. The Tax System Redesign Project (TSR) is a long-term plan to entirely reorganize the tax information data bases. The redesign is expected to take advantage of state-of-the-art systems design, software, data bases, hardware and telecommunications. Artificial intelligence concepts are expected to play a big role in the control of data bases. The IRS is presently staffing up a division to concentrate on artificial intelligence research, for applications both in TSR and AES as well as other Treasury uses. Other technologies expected to be employed are laser storage; satellite, microwave and fiber optic communications; and labor-saving devices such as Optical Character Recognition (OCR), speech recognition,and natural language processing.

Whereas the present record system keeps limited information online and the rest on archived paper copies of returns, the new system will contain all tax information in one data base. Access to all master file accounts will be online instead of batch. Artificial intelligence technology will be needed to manage such a large data base and to assist in the electronic filing that is contemplated. Rule based systems will be constructed to assist in data base updating.

Tax practitioners, and ultimately private citizens will be able to file returns electronically, first from terminals located in District Offices and eventually from home computers. Refunds and payments will be by electronic funds transfer.

Some technologies are currently being experimented with. OCR is now used for some processing. A pilot program of optical disk storage of returns is taking place in Fresno, California.

Unauthorized access will be the primary security issue for the new system. IRS officials feel that maintaining all tax information online will result in greater security overall than the present paper storage system. A request for a proposal is being issued for analysis of redesign plans by a security expert. IRS hopes to exercise even tighter security over the new data base than over the present ones.

Instead of delayed audit controls, there will be real time notice of unauthorized access. The artificial intelligence security system will assign workload inventories. Security and integrity of private electronic data input could conceivably be handled by issuing each taxpayer their own computer chip so that they alone can enter return information.

The data set will consist of only the information contained in the returns. There will be no tie-ins with other data sources, such as stock market information. No one interviewed could comment as to whether other agencies would want access to the new data base or whether such access would be allowed.

An advisory committee is being set up of persons knowledgeable about electronic data systems to discuss privacy and confidentiality issues of the system redesign plans. This committee is to be separate from the current Tax Advisory Group.

The start-up of TSR is expected to be completed in 1990. Timetables are outlined in the Management Plan for the Tax System Redesign (TSR) Project, Revision 1, June 22, 1984.

Taxpayer Service. Information about tax returns is disseminated on radio and television. Taxpayers can dial pre-recorded tapes by telephone. A Refund Inquiry File put up by the Service Centers can be queried by telephone. Taxpayers who are due a refund but who have not received it can key in their Social Security number and refund amount and track the processing of their account.

Electronic Mail. The Data Processing and Human Resources units are investigating alternatives for executive level inter-city communication of management information and administrative data. Persons involved with the Human Resources Network for intra-agency management communication are participating in the electronic mail study also. The task force is studying both the technical and policy aspects of electronic mail. The biggest issues are procedural—what should be transmitted electronically, how the transaction should be controlled, who owns the communication, and problems of authentication and "signature trail". Final decisions will be made by the Automation Policy Board, which consists of three Associate Commissioners, the Deputy Chief Counsel, the Deputy Commissioner, and three Regional Commissioners. A decision will be made as to whether electronic mail installation will be contracted out or performed inhouse. The electronic filing of correspondence is also being investigated.

Data Sharing. Section 6103 of the IRS statutes allows certain exchanges of data held by IRS. Tax administration information is exchanged with state governments.

State and local agencies participate in data exchanges in child support enforcement efforts.

DATA ANALYSIS AND SYNTHESIS

1. Constituencies Affected. The Internal Revenue Service has the largest special constituency of all the agencies studied: all corporate and individual taxpayers. Significant changes in data collection and use by this agency therefore would affect large numbers of people and businesses. Another constituency not yet addressed by this study includes IRS employees and the electronic transfer of their payroll and personnel records.

2. Public Meeting and Comment on Proposed Rulemaking. These are still conducted by traditional means. Videoconferencing has been considered, but it is not presently being used.

3. Dissemination of Publications. There have been relatively few cuts in printing and publishing at IRS. Documents consist of tax instructions, statistics of income, the Annual Report and the IRBulletin, and most are provided free.

IRS practices reflect stringent criteria on justification and clearance of publications. Also, IRS publications are integral to its mission. For these reasons they were not cut severely after OMB's moratorium on printing.

In 1984 IRS set up a pilot project to disseminate its publications online. The goal is to reduce printing costs by making documents available online and to provide convenient access to taxpayers. In February 1984, 66 publications were made available to Compuserve and BRS, and 16 to Vutron, for dissemination through telecommunications. At this stage, the precise impact on the taxpayer constituency is unclear. Most of the publication work at IRS is contracted to GPO; some to the private sector.

4. Contracts for Dissemination. This topic was not discussed at length during the group interview. The Research Division uses contractors for surveys or data compilation and for dissemination.

5. Library Closings. Not Applicable/Not Discussed.

6. Marketing. Information to taxpayers is disseminated by radio, television and telephone, as well as in documents. Research results are generally available through FOIA. In a sense, IRS is marketing to the academic community by making results on tax administration research available to stimulate interest in this area. It was not apparent from this study whether IRS marketing efforts are sufficient to

acquaint the public with the full range of publications available.

7. Personal and Company Information Rights. A tremendous amount of personal and company information is collected by IRS for the administration of the tax system. When the system is redesigned, there could arguably be an even greater potential for infringement of privacy and confidentiality rights. IRS officials claim that record-keeping by electronic means protects confidentiality more than traditional paper archiving methods. Data collection (return filing) will ultimately be performed electronically, using microcomputers, giving rise to greater security concerns. Other uses for microcomputer-mainframe links are forcing the Service to address inhouse microcomputer security considerations as well.

IRS follows the disclosure guidelines of Section 6103 and the Privacy Act. In disclosure issues, IRS will lean heavily to the data protection side. The Service has a combined Disclosure and Security Division.

Presently, account information is indexed in the master file by Social Security number, not name. When the data base is restructured, the issue of personal identifiers must be re-addressed.

International data exchanges are performed manually at present. Domestic data exchanges occur with state and local governments and agencies, and other Federal agencies. Computer matching is done with bank records and mailing lists to identify and correct nonfiling. No infringement of civil liberties was demonstrated, but the issue could bear further investigation.

8. Security Procedures. Extensive physical and logical controls are in place for computer systems. Different security considerations were addressed for online and batch systems and now for microcomputer-mainframe linkages and lap computers. Microcomputer security is being promoted as a management responsibility. Unauthorized access is viewed as the primary security concern of the proposed master file redesign. Security/privacy training is given heavy emphasis in the Collection and Disclosure Divisions.

TOPICS FOR FURTHER RESEARCH

The scope of the IRS investigation did not permit extensive exploration of all the issues, and any findings at this date will have to be re-evaluated in five years when the Tax System Redesign project is operational. Procedures currently in use and nearer completion raised the following issues:

- Results of the electronic mail task force study should be evaluated when

they are available.

o The expert systems to be used in the AutomaticExamination System could be examined for their accuracy, reliability, and effect on discretion of examiners. Also an issue raised by AES is the security of portable computers which will have access to account files.

o The Automatic Collection System could also have an effect on the amount of discretion exercised by collection representatives. Planned linkage with IDRS will raise more confidentiality issues.

o Alternative record storage means: the optical disk storage pilot project has been operational and legal and records management principles could be evaluated.

o Further research on the debate between IRS and NARS as to the archiving of taxpayer information would be interesting. IRS guidelines for electronic records management should be located and reviewed.

o Data sharing with other entities merits further examination.

4.5 DEPARTMENT OF LABOR

INTRODUCTION

The mission of the Department of Labor is to foster, promote, and develop the welfare of the wage earners of the United States, to improve their working conditions, and to advance their opportunities for profitable employment. To accomplish this mission, The Department of Labor is structured to conduct a variety of affairs dealing with labor, employment, training, labor-management relations, labor statistics, and occupational health and safety. Each of the subsections of Labor functions independently with respect to its program missions, so that the agency resembles a confederation of independent agencies which often have little to do with each other. However, these agencies are united through common administrative procedures, such as payroll and personnel.

Information technology implementations follow this organizational pattern and are operated in a fairly decentralized manner. Administrative systems, which serve department-wide functions such as personnel and payroll, are handled by the Assistant Secretary for Administration and Management (OASAM). Data systems which address programmatic functions are independent and are the responsibility of the respective Program area.

Given the organizational and technological structure of Labor, this agency profile presents a description of practices in OASAM, the Office of Information and Public Affairs, followed by a description of one of Labor's program areas: the Employment and Training Administration.

OFFICE OF THE ASSISTANT SECRETARY FOR ADMINISTRATION AND MANAGEMENT

Mission and Scope. The responsibility for Information Resources Management (IRM) for the Department is presently divided between the Directorate of Management Policy and Systems and the Directorate of Information Technology. Under consideration is a proposal to merge these two offices into one office to accomplish the IRM objectives.

Directorate of Management Policy and Systems. This office is an administrative organization responsible for developing and recommending new and revised management policies and systems; managing implementation of OMB Circular A-76

(Performance of Commercial Activities); promoting the cost-effective use of office automation in OASAM and other departmental management components; and managing implementation of the non-ADP portions of the Paperwork Reduction Act of 1980.

To accomplish this mission, this office manages several functions. One of these functions is to develop, recommend, and oversee approved policies and procedures for implementing OMB Circular A-76 and to establish and maintain required inventories of commercial activities. Another function is to develop opportunities to apply cost-effective use of office automation in OASAM and Departmental Management organizations. This office recommends system designs to solve problems for department management.

This office also develops policies for, establishes, and maintains a comprehensive internal paperwork management program of directives, records, reports, forms design and control, and correspondence management systems. The office is responsible for the authority to acquire information from the public and establishes policy on questions of whether to collect certain types of information. All forms and survey instruments must receive clearance through this office.

Another function of this office is to recommend policy and procedures for implementation of the Paperwork Reduction Act of 1980; and to monitor agency implementation of established policies and procedures for information collection budgeting, and management of information resources (excluding information technology). In this vein, this office schedules and carries out reviews of the management of information resources and information collection systems in the Department's agencies. Six to eight reviews are conducted each year.

Directorate of Information Technology. The responsibility of this office is to manage the processing of data if it is processed in an ADP environment. There are presently seven different computer environments, ranging from remote access, isolated areas to highly populated, direct access sites. Only one system is owned in-house; the other six are maintained by commercial operators such as EDS/OSI, Boeing, Martin-Marietta. Use of these large, time-sharing facilities are managed and maintained through procurement contracts with the Department which specifies the performance, operation, and security considerations of these systems.

Security. One advantage to using these large systems is that well-proven, highly sophisticated security systems are already in place and can be applied to the data files maintained by the Department. Since the Department has neither the staff nor the facilities to maintain such highly secure systems, it can share the costs of these large, time-sharing facilities across the customer base. Security includes

calamity protection, and protection from unauthorized access and use of the data. Each customer on the system is isolated; and software protection devices are in place, including password and identification code access and the use of rule sets to limit access.

Other security measures include using leased-lines to protect unauthorized access to the network; high speed telecommunication facilities (2400, 4800, and 9600 bpi); and unannounced checks and audits of the system. The systems have also been infiltrated with "check" records that can be monitored to determine if there has been any unauthorized use or manipulation of records. This office has recently published a handbook on "Security and Privacy of Sensitive Application Systems," which describes policies and precedures for ensuring the security of automated systems.

Administrative Management Information Systems. This office maintains the administrative and accounting systems, including payroll, personnel, property management, and procurement systems. The payroll and personnel systems are linked by an automated interface that allows common data elements to be shared. Staff working with these systems are trained in the sensitivity and privacy of the records during the orientation program. This training program includes information on the FOI and Privacy Acts and Departmental policies regarding privacy of records.

Matching. The Payroll system is based on the Social Security number, and matching is done against unemployment data maintained by the states. Agreements are made with each state to provide tapes of the payroll data; the matching procedures follow the guidelines authored by the Office of the Inspector General and are based on the revised OMB matching guidelines.

Categories of Technology. The Department is heavily automated with large, computerized data bases. Depending on the nature of the system, several are organized around large central computing centers with access through remote terminals at isolated sites. These systems use interactive telecomputing as part of their operations. One computer system provides electronic mail facilities; usually informal communication is transmitted, with very little formal communication using the electronic mail medium. The facsimile machine is used to transmit official documents between headquarters and the regional offices.

Microcomputers. Over the past two years, the integration and use of microcomputers has been increasing. The greatest use has been in linking them into the program systems already in existence. This presents a security problem as data

can be downloaded onto the microcomputer, processed, and returned to the main computer system without being monitored. Confidentiality and accuracy cannot be presently controlled. Changes can be made to files without immediate detection. A solution has not yet been found for this problem. Audit checks can be made but they do not offer a complete solution.

Changes in Information Practices. There have been no discernable changes in the Agency's information practices due to technology. Legislative changes have impacted the flow of information and the type of information collected. For example, the change from the CETA to the JTPA program has given more program activities to the states, resulting in a difference in the amount and kind of data collected and reported at the Federal level.

Office of Information and Public Affairs

Mission and Scope. The mission of this office is to publicize the activities of the Department. The information released by this office is targeted to the news media for subsequent release to the public. Congress is also a major target for information released by this office. This office has three objectives in accomplishing its mission. First, it advises the Secretary of Labor on matters relating to public information, and to directs and guides operations of the Department of Labor's public information and publications activities. Second, this office provides the press and other mass media outlets with materials regarding the Department and plans, organizes and conducts effective and economical department-wide publications programs. As part of this mission, this Office develops and prescribes policies, guidelines, and standards governing press releases, articles, speeches, publications, reports and similar materials prepared by the agencies of the Department. It also plans, prepares and issues departmental press releases, special publications and reports on the current policies, programs, and activities of the Department.

Third, this Office provides effective and economical audiovisual and graphic communications for the Department; and plans, organizes, conducts, coordinates, and establishes policy and guidelines for all design, graphics, viodetape, film, photography and exhibit productions. This Office also plans, develops, and executes a regional program to inform the public of the Department's policies, programs, and activities.

Access. The major vehicle used by this office for disseminating information is the news release which is available in hard-copy through the office or by mail. In matters of urgency, news releases are phoned into news media offices. News

releases are also distributed through a private news service called Press Relations Wire. Information is also disseminated on occasion (as necessary for timeliness or importance of news item) through news conferences or television statements. This office also has access to the DIAL-COMM computer network, but does not presently use this outlet for information dissemination. There is not enough interest on the part of the news media to make it worth the expense the Department incurs for use of the system. It is expected that as the major news agencies and services begin using DIAL-COMM that this office will begin to release its new items through this computer service.

Information is released to the regional offices through the telecopier services. Under consideration is the use of the Harris system, an already-established computer network linking headquarters to the regional offices. Use of this system will provide for more immediate release of news items and information to the regional office staff.

The paper files maintained by this office include news releases, transcripts of public speeches given by the Secretary, and transcripts/copies of the text of interviews or statements given to the press. These files are broken down by agency. The files are maintained for three years and given to the Department's historian for archiving.

This office also functions as the central point for distribution of publications prepared by the various agencies within the Department. It maintains a control system for publication dissemination. Other than publications from the Bureau of Labor Statistics, no publications are commercially marketed.

Trends in Information Practice. There are no major trends evident in the information practices of this Department. The tone is set by the Secretary or the Director of this office. The degree of openness depends on the individuals in these positions, but the general pattern has been to provide open access to information.

Impact of Technology. Computers will impact on how fast information can be made available to the news media and will permit a communication to be formatted in a more compatible, and hence more readily usable form. News is a perishable item; there is a great need to get the information out as soon as possible. With information technology, the outflow of information will be greatly enhanced. It is simply a matter of "marrying" the computer capabilities of the government (DIAL-COMM in particular) to the capabilities of the news media.

EMPLOYMENT AND TRAINING ADMINISTRATION

Office of Financial Control and Management Systems

Mission and Scope. It is the responsibility of the Office of Financial Control and Management Systems to undertake the procurement of ETA's program-related grants contracts. This Office provides the administrative services necessary to support these procurement activities. A master Contractor File is maintained by the Office of Financial Control and Management Systems for internal management purposes.

Under the responsibility for administering grants contracts, ETA program offices maintain 14 significant automated information systems. The "Directory of Automated Information Systems" produced by the Office of Policy and Review (Office of the Assistant Secretary for Administration and Management) provides a description of each of these systems, detailing its composition, purposes, system input and output, and the authorizing legislation. This Directory also lists the retention and disposition schedules for the records maintained on these automated information systems.

Data Collection and Access. Most of the data collection activity for these automated information systems is performed at the state agency level. For this reason, the detailed data elements do not fall under Federal Privacy Act and disclosure regulations, but are regulated at the discretion of the state disclosure laws. The data reported at the Federal level is summary data and is devoid of individual identifiers or proprietary information. Sensitivity is not a consideration because the sensitive data is not subject to the Federal Privacy Act concerns.

Staff Training with Regard to Sensitivity and Privacy of Records. Staff training follows two documents recently issued: "Assessment of Vulnerability Control," (A123), and a document recently issued by OMB on the privacy of records (OMB-71, No.1).

Risk Analysis. The Office of IRM is instituting a risk analysis program on the 14 significant automated information systems. The purpose of this program is to determine what general security measures should be instituted.

Extent of Contracting-out of Library/Information Centers. As of two to three years ago, there are no more resource centers or libraries under contract.

Office of Program and Fiscal Integrity

Mission and Scope. The responsibility of this Office is to provide programmatic and legal advice to the Assistant Secretary's Office. Acting as an in-house counsel, the Office performs audit resolution and close-out of all grants contracts. On national programs, this Office writes policy guidelines for program operations. The

investigative informaton collected in resolution and settlement of audits, including financial and tax status data, is protected from disclosure.

On request, a Special Review staff handles investigations for Assistant Secretary's office. An Internal Control Unit initiates reviews of high vulnerability programs to determine if fraud and abuse exist. Along these lines, this Unit has looked at access to electronic data bases and is working with security consultants to enhance security measures on automated information systems. Recently instituted, another unit reviews the performance of programs on a complaint basis. This review gives an objective look at program operations. The reports are presented to grantees and the program offices.

FOIA Requests. Another area of responsibility of this Office is to handle the FOIA requests that come to ETA. About 70 percent of the FOIA requests are handled through this Office, the rest go directly to the program office of concern. The FOIA requests are distributed for further response to the Disclosure Officers who reside in each Program Office. A computerized log of all correspondence including FOIA requests is maintained, and acknowledgement letters are sent to requesters indicating that their requests have been forwarded to the appropriate Program Office. For requests of special consideration or appeal, this Office provides coordination of the responses and determinations on appeals. The Solicitor's Office handles denials and cases on appeal.

The number of FOIA requests average around 250 per year. The largest number of requests comes from litigators (attorneys) representing non-profit organization or state or local governments. Other requesters include individuals and professional researchers who are researching unemployment insurance programs, employment or training experiments, or Bureau of Labor Statistics-related work.

The majority of FOIA requests have been fulfilled; the major reason for denials has been that the matter has been under investigation. Most of the sensitive data is under the auspices of the state agencies who are under grants agreements with the Federal office for data collection and processing. Requests on local, specific data are handled by the state and local offices. At the Federal level, only two areas of sensitive information exist. These are the Office of Trade Adjustment, which collects corporate or propietary data, and the Labor Certification program, which collects information about individual worker status. Limited or partial disclosure of this data would be a determination of the Solicitor's Office.

Staff Training Regarding the Sensitivity and Privacy of Data. Two seminars a year are conducted for regional and national FOIA officers. These seminars include

summary information about the kinds of requests being made, present policy and developments in the FOIA area, present status of cases and updates by the Solicitor's Office, and interpretations on policy directives.

Changes in Information Practices. The overall policy has been consistently to provide information as requested. Most of the data at the Federal level is not necessarily sensitive data that would present any problem. There have been different emphases by different Presidential administrations on reporting. President Carter's emphasis was to disclose; under President Reagan, there has been more effort made to defend against FOIA requests.

Two other issues impact the change in information practices. First, with the reductions in staff, it has been more difficult to meet time and staff requirements to fulfill requests. Second, with the increasing amount of litigation and the increasing threat of litigation, there has been more oral discussion, less written documentation. The exceptions are narrow, so there has been less documentation of various decisions, and the way the decisions are reached, in order to combat the greater chance of litigation.

United States Employment Service

Mission and Scope. This Federal office is responsible for administration of the National Public Employment Service. The office provides assistance to states in establishing and maintaining a system of local public employment offices in the states and territories. The Federal Government provides the funding for the programs and sets policy and guidelines to direct program operations. Through grant agreements, the states administer and staff employment service program activities.

The function of the Service is to provide unemployed individuals and other jobseekers with job placement and other employment services, and to provide employers with recruitment services and referrals of job-seeking applicants. To conduct this program, the state agencies must collect both personal and corporate information. Job applicants provide demographic and work history data to complete their profiles. Employers complete work orders which require that they submit corporate information.

Access. Because this personal/corporate data is collected, processed, and stored at the state agency level, the states maintain discretion over the processing and disclosure of the data. The states have broad discretion over what is automated and what is processed manually. The Federal office receives reports from the state agencies which contain aggregate data from statistical analyses, but there is no

access to the raw data from the Federal level. The states establish their own disclosure and privacy laws and prosecute for unauthorized use or disclosure. Further, the grants contracts with the state agencies prescribe federal guidelines for the protection of the data from unauthorized access, use, or disclosure.

These state agencies are monitored for fraud and abuse at the Federal level through the Office of the Inspector General. The Office of Program and Fiscal Integrity writes regulations for the programs and also reviews their operations. Any complaints directed toward the program activities are followed up by staff in the Office of Program and Fiscal Integrity.

Other Employment Services. The Secretary also has special responsibility for administering and conducting other employment service programs. Four of these programs operate nation-wide within state agencies through grant relationships. These programs are:

o Labor Certification Program, which deals with petitions to hire foreign workers or requests of foreign workers to enter the United States to find employment. The Labor Certification Office tests the need for these foreign workers.

o Target Jobs Tax Credit Program, which provides inducements (tax credits) to employers to hire targeted or special groups; e.g., veterans, welfare recipients.

o Housing Inspections Program, which provides inspections of all housing provided by agricultural employers to determine if the housing meets certain minimal standards.

o State and Local Planning Information Programs, which provide funding to states to generate state information useful to job and employment training, vocational education, etc. Publications generated from these programs are available at the state level.

Several other programs operate only in selected states. These include the Test Development Activity program which operates in 20 states under grant relationships. This program is designed to generate information relating to the validity and reliability of tests; e.g., the General Aptitude Battery of Tests. Normative data is produced from this program activity.

Five selected states participate in a program to provide occupational analysis to update the Dictionary of Occupational Titles (DOT). As new, emerging, and changing job structures are identified, they are matched against the standard coding classification system, with adjustments made to the classification as necessary.

Interstate Job Bank. The Federal Government has also financed an interstate job

bank/clearance system operated by the state of New York. When a state has a difficult position to fill, the job can be entered into the job bank for other states to access and process.

ESARS System. The Federal Government has also financed the Employment Service Automated Reporting System (ESARS) as an online system that provides ETA staff access to aggregate state performance data on employment services. This system is one of the 14 significant systems maintained by ETA to monitor the grant contract programs. The input to the system is collected at the state agency and furnished to ETA in the aggregate on magnetic tape and disk files. (The data is then input to the ETA VAX computer for further processing.) This data includes summmaries of applicant characteristics, information about services to applicants, job openings received and filled, and composite information about job types such as occupational coding, wage structure, and duration of job.

ETA staff manipulate the ESARS data using various software programs available on the VAX. Monthly and quarterly analyses are generated from the ESARS data. These reports are disseminated through the national headquarters office, the Government Printing Office, and through the individual ETA issuances.

Use of Technology. The headquarters office and the ten regional offices are linked together through a computer network. This network is used for electronic mail transfer between headquarters and regional office staff. The computer network is also used for computer conferencing; e.g., to get input on particular policy guidelines. Draft notifications are also put up on text files for review and comment by regional office staff.

Attitude Toward Use of Technology. The impact of the major reorganization of the Department and the tremendous reductions in staff have hindered the Department's ability to move ahead on technological issues. Even though there exists an awareness of technology and its capabilities, the loss in continuity in program management due to staff reductions greatly impedes the Department's ability to incorporate the use of technology. With cuts in funds available for travel, computers have been beneficial to program operations benefit program in their capability to transfer data, provide telecomputing options. Staff would like to implement more technological advancements but they are too busy re-educating or training staff in basic program operations due to staff changes and staff reductions.

United States Unemployment Insurance Service

Mission and Scope. The Federal Unemployment Insurance Service (UIS) provides leadership and policy guidelines to state employment security agencies for the

development, improvement, and operation of the Federal-state unemployment insurance system. The Federal Government provides for the proper and efficient administration of the system, and ensures substantial compliance with Federal laws and regulations governing the operation of the system. The Federal Government is responsible for establishing the boundaries and minimum requirements for the states in operating the programs. The responsibilities of the state agencies include the structuring of the tax schedule, determining benefit amounts, and establishing eligibility requirements (above Federal minimum standards).

Additional responsibilities of the UIS include providing national leadership and policy direction for programs under the Redwood Employment Act; Disaster Employment legislation; and trade adjustment assistance. The UIS also determines eligibility and ensures payment of benefits for those earning wages on an interstate basis or under combined wage (2 or more states), and for former Federal employees.

Data Collection. Data is collected from multiple sources for reports and forecasts prepared by this office. States report summary data on employment characters on a routine basis, and additional statistics are provided by Census, Bureau of Labor Statistics, and the Council of Economic Advisors. This data is used to forecast what is happening in employment/unemployment trends. It is also used to predict revenues and payments for the system.

Disclosure. The data collected by the states are covered by the state's own privacy laws which are often more stringent that Federal law. The grants and contracts with the state agencies for data collection and processing also address the privacy and disclosure concerns. Under these contracts, the state agencies agree to provide notice to individuals when disclosure is made; to protect confidentiality and security of data; and to ensure that there will be no sharing beyond appropriate use. The Department's policy level decision on disclosure is not to go one step further than the literal statement of the law.

Use of Computer Technology. Special software programs have been developed in-house with contractor assistance to prepare statistical forecasts. The software provides constructed econometric and time-series models for manipulating the data. In addition to these models, standard statistical software packages are used to generate the reports. The forecasting models are considered proprietary information for decisionmaking and are not subject to disclosure. The results of the forecasts are made available in the publications, however.

ETA has a computer system that links the headquarter's office with the regional offices. Electronic mail is used on an informal basis; not for official

business. It is a very useful system for communication. The states use computers linked by telephone hook-up to transfer data from their automated files.

The Federal office has sponsored a network between the states by making funds available to them. The Internet system was established through a voluntary arragement. Wage information (using Social Security identifiers) is shared and some statistical reporting is conducted through the use of this network.

Publications. The Unemployment Insurance (UI) Outlook is a regular publication which specifies a projection of insured unemployment. This publication is released to those Federal and state agencies and private sector users who are listed on the mailing list. On a weekly basis, a Trigger Notice is published which announces insured unemployment rates for every state and territory. Quarterly reports provide comprehensive coverage, with important details listed by state and a national summary data page attached.

Quality Control System. This system will be operational in April 1985, and will involve data collection using Social Security numbers to identify by claimant. The bulk of the data collection will be at the state agency level, but some will be under Federal auspices. Protective measures have been incorporated into the system, including scrambling Social Security numbers. The advanced proposed rulemaking for establishing this system of records has been published in the Federal Register. The notice of proposed and final rulemaking is under development and will be published. No hearings are going to be conducted; comments will be accepted in writing.

Matching. As part of the Deficit Reduction Act, there is a section which defines the Income and Eligibility Verification System. There is now a movement under way by the Inspector General community and the Grace Commission to broaden the definition that wage and income information be shared so that managers of entitlement programs can verify eligibility. This broader definition will require that the Internal Revenue Service supply on request income information by Social Security number (earned and unearned income), and the state employment agencies must supply wage information on request. The intent is to use the Social Security number to match on individual levels. Unemployment Insurance will not benefit; it will only supply information on request.

Impact of Technology. The use of computer technology has provided greater access to information and greater capability in providing better forecasting analyses. It also has decreased the amount of time it takes to respond to questions and requests from the Congressional Finance Committee and from state legislators who need

immediate feedback. The national office is also providing a new program called the Benefit Financing Model which provides data analyses and forecasting reports on state-specific data and according to state-specific laws. Twenty states are now using the program, with five more states to join within the year.

National Occupational Information Coordination Committee

Mission and Scope. The National Occupational Information Coordination Committee (NOICC) is charged with several major responsibilities in fulfilling its mission. First, NOICC with the use of program data and employment data, shall improve coordination and communication among the developers and users of occupational information. Second, NOICC shall develop and implement an occupational information system to serve the needs of vocational education and employment and training programs at local, state, and national levels, with special attention given to the labor market information needs of youths and adults. Third, NOICC shall conduct studies on the effects of technological change on new and existing occupational areas and the required changes in knwoledge and job skills. Fourth, NOICC shall conduct research and demonstration projects designed to improve any aspect of occupational and career information systems. NOICC shall also provide technical assistance to state and local agencies in the development of information programs, including programs for online computer systems and other facilities which provide career information at sites such as local schools, public employment offices and job training programs, and programs for developing, maintaining, and using occupational supply and demand information systems. To accomplish these objectives, NOICC has administered grants programs to states to develop and maintain career and occupational information systems and programs. The counterpart to the NOICC are the State Occupational Information Coordinating Committees (SOICCs).

Statewide Career Information Delivery Systems (CIDS). NOICC has supported through grants programs the development of statewide career information delivery systems. The systems deliver national, state, and local information and provide a resource for vocational and career education programs, career and employment counseling, job placement, and educational planning. The financing of a the CIDS is complex, with resources coming from local user fees, state-level fundings, and Federal grant funds.

These information systems use data and information available through numerous state and Federal agency programs that collect labor market, occupational, and educational data. CIDS provides information about occupations, occupational

clusters, education and training opportunities, and other subjects appropriate to vocational guidance and career explorations. The states develop their respective information systems according to the amount of money and information available to them.

Access. CIDS delivers information through a variety of means, such as online computers, microcomputers, printed materials, microfiche, and in some instances a toll-free telephone hotline. The early CIDS promoted use of mainframe computers with access throughout state via remote terminals. As costs went up and facilities expanded, these large systems became expensive to maintain. With the advent of more powerful, yet inexpensive microcomputers, there has been a decided movement toward microcomputer delivery of CIDS. Where electronic access is not available due to budget constraints or otherwise, there is an attempt on the states' part to minimize the limitation and provide other access modes, usually through hardcopy. Increasingly, the states are providing printed materials, incldding tabloids containing information about occupations, occupational outlook, and educational and training opportunities.

Marketing. This involves advertising, promoting, and selling the CIDS to school adminsitrators, counselors, and managers in diverse agencies--both public and private.

Occupational Information Systems. The Occupational Information Systems (OIS), developed at the state level under direction and funding from NOICC, is used for program planning and decisionmaking, and career counseling. The potential users of the OIS are categorized as direct participants in the labor market, labor market intermediaries, such as persons who assist others in preparing for the world of work, and planners and administrators who develop and implement job-related education and training programs.

The OIS consists of four data components and one analytical component. The data used for the OIS is gathered from other going sources of information and other information systems.

o The Occupational Demand component contains information pertaining to the number of job opportunities in speicfic occupations with a specific geogrphic area over a given period of time. This information is collected from such agencies as Census, the Occupational Employment Statistics Program, the Employment Security automated Reporting System.

o The Occupational supply component consists of information pertaining to the number of individuals who are working, or seeking work, in specific occupations

within a specific geographic area over a given period of time. The sources for this information include Census, ESARS, and Unemployment Insurance data sources.

o The Occupational Characteristics component contains information pertaining to the requirements for working in specific occupations, and general description of the occupations. Information is also provided on the characteristics of individuals who work in a specific occupation. The sources of this information are numerous and include BLS area wage surveys, Census, ESARS, industry wage surveys, and ETA and SESA publications.

o The Complementary Information component contains miscellaneous information necessary to support planning, career guidance, or placement.

o The Analytical procedure component contains the information necessary to relate occupational supply data to occupational demand data and to conduct any necessary analysis.

NOICC promotes the use of publications, with most states producing hard copy of the data to be disseminated. Maine developed an OIS for a mainframe computer system and made the documentation available for other states to implement the system. Now, a microcomputer version of the OIS has been developed. NOICC has put out competitive grants for states to adopt these smaller systems. About 20 states are using the microcomputer systems. Data is more easily maintained.

Data Sharing and Disclosure. The OIS depends on the use of data collected by other organizations and agencies. It is NOICC's policy that data sharing and disclosure follow the guidelines established by the originating agency.

Conferences. To foster communications and coordination among state committees, NOICC sponsors annual conferences to annoúce grants, changes in policy and provide a forum for discussion. With travel budget cuts, NOICC has considered other alternatives, including teleconferencing. Phone conferences have been used at various times to provide for discussion and questions.

A special project has been funded to the state of Hawaii to implement an inservice training program. Audio visual materials have been developed and sent to the Trust Territories to provide training to counselors there. Via satellite between Hawaii and the Pacific Trust Territories, staff will use teleconferening to provide technical assistance and answers to questions.

Electronic Mail. A pilot project is underway to link the national office and 15 state offices together using the ADVONET system, a vocational education netowrk. It is hoped that this network will allow electronic mail and information transfer between the national and state offices. Problems may develop, however, at the

state level, where not all state offices are in the same building or in close proximity to the ADVONET system access points. The question is how efficient the use of this system will be considering the problems of access.

Cross-Classification System. NOICC is providing the technical assistance to develop a cross-classification system of military specialties with civilian occupations. There have been grants to eight states to allow this information to be incoporated into career information systems. A proposed consortium arrangement will allow 26 states to tap into one automated information system with the cross-classification system capabilities.

DATA ANALYSIS AND SYNTHESIS

To fulfill its mission, the Department of Labor conducts a variety of affairs dealing with labor, employment, training, labor statistics, and occupational health and safety. Each component of the Department operates independently with respect to its program mission, so that the agency resembles a confederation of independent agencies. Due to the budgetary and time constraints of this project, no attempt was made to profile the information practices and impact of information technologies on the agency as a whole. Instead, a description of the Office of the Assistant Secretary for Administration and Management and the Employment and Training Administration has been presented.

Several criteria were developed in this study to assess the implications and impact of the use of information technology on agency practices in three areas of civil liberties. These three areas were access to rulemaking, provision of public information, and personal and corporate information practices. These criteria have been applied to the use of information technology for the OASAM and the ETA. Conclusions drawn from these criteria reflect only the information practices of these two components of the Department. Future studies may address the issues for other Departmental components, in particular the Bureau of Labor Statistics.

Constituencies Affected. The first criterion concerns the constituencies that are affected by agency policies and practices, especially those involving the use of information technology. The Department of Labor, and specifically the OASAM and the ETA, serve a wide range of constituencies. These agencies serve the concerns of the employed and unemployed in the labor force. The agencies' programs are targeted to servicing the unemployed and job seekers with job placement, career information and employment services, and employers with recruitment services.

These agencies also provide business and industry with statistical reports and forecasts of labor market activity. Through grants contacts, these agencies also interface with state and local agency staff in data collection and reporting of labor-related statistics.

All these constituencies have benefited from the increased use of information technologies. Automated information systems provide more up-to-date job placement and career information to job seekers and those changing careers, and supply business and industry with more accurate and timely statistical reports and forecasts of labor market activity. The computerized statistical and mathematical manipulation of this data is far superior to manual techniques. The use of the microcomputer has also made it easier for state and local agencies to provide occupational and career information available at lower cost. Yet, it is still the concern that all constituencies be served, even those who cannot afford (micro)computer access. The agencies continue to use alternative methods of information dissemination in their efforts to serve all constituencies.

Public Meetings and Comment on Proposed Rulesmaking. Technology has not changed the number or type of public meetings held by OASAM and ETA. Notice of hearings is still accomplished through the Federal Register, and public comments continue to be submitted through conventional means. That practice is expected to continue. Only one organization, the National Occupational Information Coordination Committee, has addressed the use of teleconferencing as a means of facilitating the participation of interested parties in the training sessions and national conferences.

Dissemination of Publications. Publications are distributed through the program offices, the Office of Information and Public Affairs, and the Government Printing Office. Many of the programs funded by the Department are carried out by state and local agencies, and much of the data collection and dissemination is accomplished at this level, with Federal funding and guidance provided through the grants agreement. Even though the state and local agencies use computer technology for data base management and for disseminating public information, there is still the concern that this information reach all constituencies, even those which do not have computer access. The National Occupational Information Coordinating Committee, in particular, has addressed this issue and has made it their policy to direct the state and local agencies to make the information available through alternative modes of dissemination, either through audio visual materials or hard copy publications.

Library Closings. The Office of Financial Control and Management Systems (ETA) indicated that as of the past two to three years, there have been no more resource centers or libraries under contract. Budget cuts were cited as the reason for this.

Personal and Company Information Rights. Through grant agreements, ETA funds state and local agencies to operate most of its programs, including the data collection and reporting activities. For this reason, most of the data is considered under the purview of the state agencies and does not fall under the concerns of the Federal Privacy Act. The states have enacted privacy laws which cover the unauthorized disclosure of this data, and the laws are often more restrictive than the Federal Privacy Act. Concern arises, however, when the Federal and state laws conflict.

Another concern is the practice of sharing data among different agencies of the Department, and other state and Federal agencies. The state occupational information systems compile statistics from several sources, including the Bureau of Labor Statistics and the Employment Service Automated Reporting System (ESARS). Labor market forecasts are prepared from statistics compiled from BLS, Census, and the Council of Economic Advisors. While the data being shared is summary data from statistical reports, it represents highly sensitive personal and corporate information. The concern remains that protection against unauthorized access and disclosure be maintained in these data sharing projects.

Computer matching is another issue that could present potential problems for the privacy of personal and company informaiton. The Payroll system in OASAM submits data for matching against unemployment data. This matching probject follows the OMB matching guidelines. Another project involving the Unemployment Insurance Service is to broaden the definition of the income and eligibility verification system and allow matching of wage and income information to verify eligibility for entitlement programs. Matching will be done on Social Security number and will include wage and income data from the Internal Revenue Service as well. The Director of the Unemployment Insurance Service expressed concern that scope of this matching project may be too broad and constitute an infringement on personal and corporate information rights.

Security Procedures. The computerized information systems used by OASAM and ETA are protected by security built into the computer systems design. At the minimal level, there is password identification code protection. At a higher level, rule sets are built into the software programs to limit access to files and systems. On the larger time-sharing facilities, security protection is maintained by highly

sophisticated security measures, which include calamity protection and protection from unauthorized access and use of the data.

The use of microcomputers and stand-alone systems presents a bigger problem for security. While the problems are under consideration, no solutions have been implemented. Further study is needed to overcome the problems of security for microcomputer use.

4.6 SMALL BUSINESS ADMINISTRATION

INTRODUCTION

The Small Business Administration (SBA) derives its authority from the Small Business Act (15 U.S.C. 631 et seq., 1953) and the Small Business Investment Act (15 U.S.C. 661, 1958). The basic mission of SBA is to protect the interests of small business. SBA is allowed to license, regulate, and make loans to small business investment companies. Both direct and guaranteed loans are made to small businesses. Disaster loans can be granted to homeowners and were until recently given to farmers. One of SBA's fundamental purposes is to ensure that small business concerns receive a fair portion of Government purchases, contracts and subcontracts, as well as of the sales of Government property. Various agency programs have been set up to provide counseling and assistance to small business owners in general and within specific special interest groups: minority-, veteran-, and women-owned businesses.

SBA could be described as an agency on the brink of automation. Information technology is currently used primarily in the form of internal tracking systems. The principal data collection activities, loan applications and management, are initially gathered in paper form but entered, maintained and manipulated online. Information dissemination, and public access to rulemaking, are still conducted by nonautomated means. A discussion of these and other issues follows in the profile of SBA. Information handling procedures are described for each organizational unit, followed by an analysis of civil liberties implications.

FREEDOM OF INFORMATION/PRIVACY ACTS APPELLATE OFFICE

Mission and Scope. The FOI/Privacy Acts Appellate Office handles appeals on denials of requests under both acts made by officials of any field office or division, or by the Central Office.

Freedom of Information. Initial FOI requests come in to FOI officers or general counsel at the regional, branch and District Office levels. Requests also come in to many of the offices within the Central Office. Those coming in to this office are passed on to the appropriate division, but are still followed up through a "tickler" system.

The branch offices are the smallest which can receive an FOI request. They

may send them on to the District Office or have their branch counsel handle the request. At the District level, 80 percent of the offices have FOI Officers and the remainder employ their own counsel for handling requests.

There are no figures on the amount of FOI requests made because of the wide number of sources. The FOI Annual Report for 1983 shows that 388 initial denials were made.

Requests are generally from competitors who want to know why X Company got a loan and how they qualified. The Inspector General's office receives a large number of requests for audit and investigations files, which they will turn over if there is no pending investigation or litigation. One hundred and fourteen denials were made by the Inspector General in 1983.

Once a request has been denied, the requester has the right to appeal. Ninety-four appeals were acted on by the Appeals Office in 1983, and 22 were reversed and disclosure granted. The director rules on all appeals taken to his office. Besides the director, the staff consists of three FOI specialists and a clerk.

SBA SOP Standard Operating Procedure (SOP) 40 03 1, Disclosure of Information, January 11, 1983, states that the SBA policy is to disclose requested records even if they are exempt, so long as no other law is violated or any legitimate public or private interest harmed (p. 21). The principal laws upon which disclosure may be denied are the Privacy Act, the Trade Secrets Act, and the Right to Financial Privacy Act (12 U.S.C. 3401-3422, 1978). In 1983 denials were also made under the authority of Internal REvenue Service statutes.

Staff Training. The FOI staff receives training from many different sources on the confidentiality issues with which they must deal. The Departments of Justice, Agriculture and Labor all provide training. Different non-governmental law associations also conduct training sessions. The FOI/Privacy Office gives the inhouse training on confidentiality issues for divisions of the Central Office that often handle FOI requests, such as the Portfolio Management Office and the office of the Inspector General.

Personal information contained within SBA files can consist of the personal history statement in the loan file. (See regulations 13 CFR 102.3 for a list of personal/company information that is exempt from disclosure.) The FOI/Privacy Officer stated that more information about actual data could better be obtained from other sources within the agency. Company information that would be considered confidential and exempt from disclosure under the FOIA exemptions are such records as financial statements, credit reports, requests for size determinations

and license and loan applications. (See SOP Disclosure of Information, p. 26)

Privacy Act. There is little use made of the Privacy Act for requests by individuals to see records maintained on them, other than for personnel matters. Most personal information maintained by the SBA, such as the personal history statement, is directly collected (volunteered) by applicants. The Appeals Office uses (as does the whole agency) SOP 40 04, Privacy Act Procedures, 9/27/75. Initial requests are generally made at the local and division level. The Privacy Act does not provide for appeals, but SBA has set up an appeal procedure exactly like that under the Freedom of Information Act. The Appeals Office is notified when records under the Privacy Act are disclosed, but the Office does not monitor the notifications.

SBA also uses the System of Records Index which lists record systems that fall under the Privacy Act. For each record, there is listed categories of information taken from the Act, routine uses and users, access procedures, retention and disposal guidelines, record sources and named managers. This index does not have the weight of an SOP but serves to put the employee on notice. If a record system does not meet the criteria of a nonexempt system, then any disclosure must be carried out under the Privacy Act Procedures.

The Privacy Act Officer (PAO) receives a statistical log of all disclosures that have been made. The PAO is also responsible for compiling an annual report on systems of records maintained by SBA, as required by the Privacy Act and its implementing regulations and guidelines. The 1983 report shows 66 active nonexempt systems and 6 active systems that are exempt from disclosure. No computer matching of files is undertaken.

When the annual report is produced, the goal is to reduce the number of systems of records. To that end, there is an annual review of data collection forms which is performed by the Appeals Office staff and reviewed by the director. Not every system is reviewed every year--there is a different area targeted for review each year. Notice is sent out to all divisions to review all systems of records and try to combine or delete some of them. Proposed changes are sent over to the PAO for approval.

Technology Use. The Appeals Office has for the past six months used a Wang word processing system for tracking and storing FOI appeals. The record contains only internal processing information, not any information that could be construed as confidential.

Agency-wide, there is a new key word system for accessing files.

Changes since 1976. There have been many computer changes both in security and data base management, which are discussed below in the profile of SBA Automatic Data Processing offices. The word processing capabilities of the FOI Office, mentioned above, have also been a recent change.

There is greater communication between the agencies about FOI issues since the Justice Department has set up an attorney-of-the-day to answer FOI questions.

There is increased use of the telex to communicate with the field offices. The Freedom of Information/Privacy Act Officer uses the telex mainly to grant or deny permission for SBA personnel to testify, usually in Inspector General cases or where the existence of a loan is material to the case. The SBA is usually not a party to a suit. The officer also uses the telex to inform personnel of subpoenas that have been received for them by the Freedom of Information Office (3-6 per day).

OFFICE OF THE GENERAL COUNSEL, SBA CENTRAL OFFICE

Freedom of Information/Privacy. This office does not get requests under either act very often. If the FOI/Privacy Act Officer in the Office of Hearings and Appeals has a legal question, it is handled by the Office of the General Counsel. Opinions are issued by memorandum or phone. Occasionally counsel in the field calls for advice but there is no structured procedure for obtaining approval for their decisions.

The attorney who has primary responsibility in Privacy Act areas must agree on any notices of new systems that are published, but actual publication is done by the Legislative Counsel. Rules and regulations that are promulgated having any bearing on FOIA/Privacy must be cleared by the same attorney.

Access to Rulemaking. The Office of Legislation within the Office of the General Counsel has the primary responsibility for providing substantive public access to rulemaking. All regulations, rules and notices of proposed rulemaking are drafted in this office. The physical details of publication are taken care of by the Office of Administration, which transmits paper copy to the Federal Register. The substance of proposed rules is composed by officials in the various program areas.

The Legislative Counsel functions as advisor to all program departments on the consequences of proposed rules. Questionnaires about information necessary for the Regulatory Impact and Flexibility Analyses are also prepared by this office and sent to program staff. After editing by the OGC, the Analyses are put out by the

Administrator as a preamble to the regulation.

Comments on proposed rules go to the person named in the Federal Register, usually a program person but sometimes the Legislative Counsel. It is the responsibility of the named person to collect and analyze all comments received. When a program person is named, all comments are shared with the Office of the General Counsel for legal analysis. There are no plans to allow comment on proposed regulations by electronic mail.

The Legislative Counsel also has duties under the Paperwork Reduction Act. The attorney fulfilling this function must approve data collection forms, which are then sent through the Paperwork Management Branch of the Office of Administration, and then to the OMB.

Extent of Computerization and Future Plans. The OGC currently rents Wang work stations for word processing. They also have a Lexis terminal for legal research. The plan is to switch the work stations to personal computers and continue the same word processing functions with added tracking and other MISs.

INFORMATION RESOURCES MANAGEMENT BRANCH

Mission and Scope. The Information Resources Management Branch has ultimate responsibility for information flow at SBA. The information collection budget is managed by this branch. All directives, forms, reports, records, delegations of authority and micrographics are controlled from this office. The branch chief is the designated official who must carry out agency responsibilities under the Paperwork Reduction Act.

Information Resources Development Section

This division of the IRM Branch handles the paperwork and data collection elements of Information Resources Management. The staff consists of three management analysts and a secretary. All analyses of agency IRM functions are carried out here under the direction of the Branch Chief. They must coordinate with the Legislative Division of the Office of the General Counsel on regulations that pertain to this area. Documents of any nature to be published in the Federal Register must be reviewed for authorized format.

Records Operations Section

The Records Section, which presently employs four management analysts, is in the process of being mostly contracted out under A-76. The Fiscal Records Division will continue to be controlled inhouse. The Central Records Division,

which is basically a correspondence file of the Central Office, is being decentralized under a contract.

All records management is conducted under the guidelines of the Records Management by Federal Agencies Act.

A contract was just signed to microfilm all loan accounting information, both active and archival. Pilot micrographics programs are being set up in the regions.

Extent of Automation. Microcomputers are in use throughout this branch. Word processors were traded up for PCs, which are going to be used for maintaining indices to directives, forms and reports. This is an ongoing automation project. The recordkeeping operation is to be automated also--information that the branch maintains about directives, forms and reports will be accessible by computer.

A contractor is currently developing a file for the microcomputers that will generate computer output microfilm. Computer retrieval of microfilmed documents is also planned.

Information Resources Maintenance Section

Small Business Information Staff (Reference Library). The agency library comes within the jurisdiction of the IRM Maintenance Section of the Information Resources Management Branch. The Small Business Information Staff consists of one librarian and a library technician. There are no plans to contract out any of the library functions since it is small and easily managed by two people. The collection consists of 5,000 volumes and 160 journal subscriptions. No more than 250 titles are added each year. Legal materials are contained in the Law Library, which is not open to the public.

For a small library, the Information Staff handles a large and varied volume of information requests. No statistics are kept on numbers of persons calling or walking in, but the librarian reports heavy public use. The population served by this library consists of all the SBA field offices, banks and small business associations from Canada, other Federal agencies and councils, members and staff of Congress, students, contractors, small business persons, press, and private sector organizations such as trade associations, banks and insurance companies.

Reference service consists of Interlibrary Loans, referral to other departments of the Central Office, the compilation of bibliographies and instructions on use of the collection.

Extent of Automation. The library subscribes to the Dun & Bradstreet credit report service. Searches on this data base are run for staff members only. There are plans to install OCLC and Dialog. The collection catalog is a manual system.

OFFICE OF COMPUTER SCIENCES

Data Base Administration Staff. The Data Base Administration staff is responsible for the selection, installation and maintenance of the data base management system employed by SBA for their Sperry mainframe. Although computer security is maintained by others within the agency structure, the Data Base staff is charged with the duty of controlling its integrity, privacy and access, within the context of the Privacy and Freedom of Information Acts. (SBA Office of Computer Sciences Policy and Standards Manual, p. 4).

The physical structure of the data bases are designed by this office, based on the evaluation of information need done by the Information Systems Branch of the Office of Computer Sciences (OCS).

Within the DMS 1100 package that is the primary concern of this office are the following data bases: 1) Loan Accounting and Loan Collection; 2) Management Assistance; and 3) Security. A fourth, Surety Bond, will be up soon. All loan information kept by SBA is contained in the Accounting and Collection file. There are other data bases within the data base management system but they are subsets of the first file. For example, the Portfolio Management Query file allows loan officials in the field to determine the payment record of a specific loan. The Management Assistance data base consists of records of counseling and training performed under the auspices of MA. The Security file is an access control mechanism: persons seeking to enter the system must first go through this transaction file.

Other files on the mainframe, but not contained within the DMS 1100 package, are the Loan Account Tracking System (LATS), personnel files, information from the Minority Small Business (8a) program, administrative accounting files, and the Computer Internal Control and Review file.

Presently, all payments on SBA loans are sent to the Denver District Office. When an officer in the Denver Office wants to update the loan file, the information is entered by him/her into LATS. The Transaction Interface Package (TIP) does the processing of the many inputs from LATS, integrates them and coordinates access to the different data bases within the system. Thus the updating process is done in a structured environment, a process which allows the OCS to maintain ultimate control. Loan approval information is entered the same way, except it is done at each District or at least Regional Office on a dumb terminal. No computer record

is kept of loans denied.

DMS 1100 allows data to be brought up in specified formats but persons in the field cannot format to suit their own needs. Partly to make data available in forms more useful to local SBA staff, the agency has started a pilot project using a Data General minicomputer.

Ultimately each region will have a minicomputer which will contain a subset of the data that pertains to that region only. The field office terminals will be replaced with microcomputers. It will not be a pure distributed processing system, in that all updating will continue to be done on the mainframe and the results will be downloaded to the minis. The field officials will have a more versatile computer system, while allowing OCS to maintain a controlled environment for data handling. Data integrity and greater security against unauthorized access will be more easily maintained. Data transmission functions will still be handled by the mainframe.

The Central Office and the Washington District Office have the first minicomputers of the pilot project. The data subset consists of the loan accounting and statistical information most frequently requested by agency officials and the general public. The record (384 characters) is shorter than that used by the mainframe files. There are plans to also keep Management Assistance and Surety information on the minicomputer.

Information Systems Branch. This branch determines the information need and basic requirements of users of the SBA computer system. The Chief of Information Systems has 23 SBA employees, including two section chiefs, and 40 to 50 independent contractors. Both maintenance and development of information systems are contracted out, with the branch providing technical oversight. Information Systems Branch is also responsible for maintaining all official SBA statistics, and for preparing replies to all internal and external requests for data.

Freedom of Information/Privacy. Most requests for information, whether they are FOI requests from the public passed on by field offices or simply information needed by SBA officials in the field, are filled by one systems analyst in the Information Services Branch. The Freedom of Information/Privacy Officer forwards requests to the Director of the Office of Computer Science (OCS). They pass from the Director to the Chief of the Information Systems Branch and then to the analyst. The analyst then gets the data or provides a cost estimate if the request is large. An example of a recent inquiry involving a large amount of data was the Washington Times' request for information on all energy loans made by the SBA. Field offices may ask for lists of loans to be used in a mailing, for instance. OCS

will send mailing labels or printouts. By order of the Director of OCS, all letters authorizing the release of information, even simple field office requests, must be approved by the Freedom of Information Officer.

When other divisions of the Central Office need computer runs, they must file a written request. However, information is released without the involvement of the FOI Officer.

Information that can be accessed is typically the following: loan number, borrower's name (usually the business), Zip code, type of business, state and county codes, field office approving the loan, type of loan, agency program under which the loan comes, minority or veteran's status, and sex. Although the record contains the borrower's Social Security number, access is never gained on that field.

The Information Center. As part of the pilot minicomputer project, an Information Center has been set up by a team working under the Special Systems Section of the Information Systems Branch. The center, which opened in October of this year, was set up for several reasons. Under the previous timesharing system, it took at least a week to respond to ad hoc information requests from the public and from Congress. Use of the mainframe system for this purpose, which requires COBOL programming to generate some ad hoc reports, slowed down all the information functions of the agency. Now all FOI and Congressional reports are run on the Data General minicomputer.

The Information Center is also used to provide training and an environment for users to do their own routine, noncomplex reports, either on the mini or downloaded to one of the number of microcomputers maintained at the Center. New procedures for FOI requests are being developed by the Information Center team to make users aware of their responsibilities under FOI and Privacy.

Perhaps most importantly, the center serves as an educational vehicle where agency personnel may become acquainted with information technology. Each program office is allowed to decide which of their staff will be trained for use of the mini- and microcomputers, but the intent of the center is to be a resource for the professional staff of each program.

Presently, access to the minicomputer is controlled by a card entry system. The goal is to develop a good base of experienced users before access is expanded. Once the analysis of the pilot program is complete, the program will likely be expanded to allow some offices to use their own microcomputers to tie in to the Information Center system.

Administrative and Accounting Section. The chief of this section is responsible for SBA compliance with reporting requirements of the Debt Collection Act, and OMB Bulletin No. 83-21, 1983. This act authorizes the release of delinquent non-tax consumer debts to private sector credit reporting agencies.

Some controversy has arisen as to the limits of applicability of this law. The SBA has two contracts to transfer this information at present. All commercial debts (including farm disaster loans) and their status (current or delinquent) are reported quarterly to Dun and Bradstreet and TRW Credit Data, reporting agencies that were selected by OMB. They can download the information to smaller credit bureaus. When the project moves into its second phase, if it does, the quarterly report will also include all charged-off loans (loans which are judged uncollectible). In the third phase, the project will report delinquent consumer loans. Consumer loans administered by SBA are primarily homeowner disaster loans.

A second contract involves the quarterly reporting to Dun and Bradstreet of the Government Assistance Reports File, which consists of all business loans of whatever status (charged off or paid in full) that were not reported under the first contract.

About $230,000 worth of loans are reported under the first contract and another $50,000 under the second. Reporting is done by shipping magnetic tapes of information taken from the Loan Accounting Data Base.

This program has engendered controversy from different sources. The process has helped in the collection of loans even in the short operation of the program, which was in planning since November 1983, and has been in operation since August 31, 1984. Naturally, borrowers in delinquency would prefer that the information not be released. Banks which give out loans guaranteed by SBA have tried to prohibit the release of information. SBA uses loan status data sent by these banks in the updating of SBA's Loan Accounting File, which in turn is used to produce quarterly reports to the credit agencies. The accuracy of this data then depends upon the accuracy of the bank's recordkeeping. If a borrower claims that delinquency information is incorrect, his first recourse is to the credit agency. SBA's Office of the Comptroller, the agency's official keeper of records, will then be asked to certify that the information is correct. If incorrect data is discovered, it will be changed.

Loan status data on SBA direct loans is maintained by the Portfolio Management Divisions of the field offices. The accuracy of this information is assured by the Central Office's procedures for the entry of data into the computer

system, as discussed above.

Network Systems Branch. Communication between the field and the Central Office is carried out under the SBA Data Communications System (SBADCS). Responsibility for the acquisition and maintenance of the system lies with the Network Systems Branch. This branch also has authority over the word processing systems of the agency. Word processing support was practically nonexistent for some time recently, due to budget cuts and reductions in force. The agency is in the process of building up their word processing function. Within the Network Systems Branch, the Network Development Section has the practical responsibility for the maintenance of the nationwide computer and data communications network. They obtain and supervise contracts for installation and maintenance. These responsibilities will continue when the terminals presently in use in the field offices are replaced with microcomputers. A unit of this branch also functions as a troubleshooter for any breakdowns that occur in the communications system.

The electronic mail system is called MTS, for Message Transmission System. MTS was used for sending out policy instructions, notices from the Administrator to Regional Administrators, press releases, and scheduling. In the last two years, the use of this system to transmit policy instructions to the field has been curtailed. Memos are no longer considered official policy. To be official, a matter must now be contained in the SOPs or in an SBA Notice (an interim SOP). A new telefacsimile system is now used for the transmission of duplicate copies of official instructions.

Computer Security. Although the Data Base administrative staff is responsible for the control of the integrity, privacy and access to the data bases, the Information Systems Branch is charged with developing the internal application security features such as passwords. The OCS Security Officer is under the Plan, Standards, and Project Control staff, a group which acts largely in an administrative support capacity for OCS. Security concerns in the day-to-day operation of the office are handled by the Security Officer. He is working with the Information Center team to develop guidelines for the operation of the minicomputer. Security policies for the whole agency are set by the Computer Security Program Manager in the SBA Inspector General's Office.

Security is provided by the following: 1) physical security is by means of a card entry system in the computer room, the Information Center, the Network Systems Branch, and the Wang Word Processing Center; 2) the Terminal Security System (TSS) of passwords and user identification numbers; 3) the data base

managements system; and 4) the Network Transaction System, which is a decentralized system for authorizing terminal use in the field.

The Computer Security Program Manager issued SOP 90 25, Computer Systems Security, in 1980, under the authority of OMB Circular A-71, Transmittal Memorandum No. 1, "Security of Automated Information Systems." It is presently being revised to accommodate technological changes, as well as new knowledge of management and security principals. Changes in the document will also come about as a result of new linkage between Transmittal Memorandum 1 of A-71 and OMB Circular A-123.

A-123, Internal Controls Systems, provides guidelines for the implementation of the Federal Manager's Financial Integrity Act of 1982, which requires heads to establish administrative controls over all funds and assets of the agency, including loan money. A-123, revised in August of 1983, is not explicit about ADP controls. Agencies must conduct a vulnerability assessment, which is a different procedure from the risk assessment required by A-71. In October of 1984 OMB reviewed SBA's procedures under the Financial Integrity Act and found that they had established good programs of implementation. SBA SOP 00 021, Internal Controls Systems, was written to cover ADP controls as well as manual systems, to eliminate the reporting of duplicative assessments to OMB.

The SBA risk assessment concluded that computer security was more necessary to protect against "fraud, waste and abuse" than any violations of privacy. SBA computerized information is generally not confidential. SOP 90 25 lists the following types of information considered to be sensitive or critical: 1) data protected under the Privacy Act; 2) confidential business information not releasable under FOIA or SBA Regulations; 3) automated decisionmaking applications; 4) sensitive financial systems; 5) personnel and payroll systems; and 6) other (p. 13). There are no grades of sensitivity as in other agencies.

Program managers are required to identify sensitive data within their divisions. Information considered sensitive or critical is protected "aggressively."

Computer Matching. At present, there is no computer matching program in existence at SBA, nor are there any plans for such a program. The agency recognizes the potential for abuse: a person could collect a loan in one region, change their name slightly and collect another in a different region. Computer matching could not detect a changed name and social security. Several years ago there was a project which matched Farm Disaster loans administered by the Department of Agriculture against SBA disaster loans to determine the identity of

any recipients of duplicate payments. This match will not be repeated since SBA authority for farm disaster loans was transferred to the Farmer's Home Administration in 1980.

OFFICE OF ADVOCACY

Mission and Scope. The Office of Advocacy was established to represent small business within the Federal Government. The Office head, the Chief Counsel for Advocacy, must act as the spokesperson for small business, measure the impact of regulation on small entities, and inform the small business community of issues that affect it.

OFFICE OF INTERAGENCY AFFAIRS

In addition to assisting entrepreneurs with any problems in dealing with the Government, this office monitors Federal Agency compliance with the Regulatory Flexibility Act.

OFFICE OF ECONOMIC RESEARCH

This office coordinates and conducts applied research on a variety of small business issues. These studies give Advocacy a factual basis for the formulation of its policy arguments. Economic Research is developing a data base that can be used to determine trends and conditions of the small business community or a sector thereof. Annual statistics on employment and sales, and balance sheet information are included.

OFFICE OF INFORMATION

The Small Business Administration Act stipulates that the Office of Advocacy must communicate with its constituencies of small business persons and organizations, other Federal officials, and Congress. The Office of Information is responsible for much of this communication. Small business issues are analyzed in publications such as Advocacy Current Topics, Small Business Research Summaries, and Advocacy Issue Briefs. About 200-250 publications per year are issued by Advocacy, including pamphlets and a small business newsletter called Advocacy

Notes. Most are written and edited within the Office of Advocacy and printed at the agency printshop. A portion of the publications are sent out to GPO. Advocacy publications are not actively marketed.

The office staff consists of four full-time secretaries and three full- time professionals. Everyone responds to telephone inquiries. The professionals issue press releases and write, edit and proofread publications.

Thirty or more telephone calls are received per day. Most callers request Advocacy publications or information about the various programs run by the office, such as the Small Business Person of the Year Award, and a poster contest. Questions about other agency functions or regional areas of expertise are referred to the appropriate offices. Publications are also distributed to requesters who write for information. Only Advocacy publications are disseminated by this office.

SMALL BUSINESS ANSWER DESK

The SBA maintains an information and referral service with a toll-free number within the Office of Advocacy. Three operators staff the Answer Desk. They receive between 200 and 300 calls per day. Persons requesting publications are referred to Advocacy, Management Assistance or Public Information, depending on the need. General information questions are answered by the Desk staff or referred to other offices.

OFFICE OF PUBLIC COMMUNICATIONS

Mission and Scope. The Office of Public Communications (OPC) provides general information to the public, the press and other agencies. Within OPC, the Publications Office produces publications for each program area as well as internal SBA materials.

OPC receives approximately 15 telephone queries a day from the public and other agencies. Less time is spent answering questions from the press. Press questions are researched and the information forwarded to the reporter. OPC maintains a working relationship with one Washington Post reporter to whom they supply press releases. News is also released to UPI and AP.

Telephone inquiries are of all types, including practical questions such as how to start a business, general information about SBA, descriptions of SBA programs, and requests for publications. If the caller asks for publications available to OPC, like program area descriptions, press releases, or proposed regulations from the

Federal Register, OPC staff will pull the information and mail it out. General information questions are often referred to the District Office or to the Publications Office within OPC.

PUBLICATIONS OFFICE

Internal SBA publications consists of a weekly letter and packet of information to Public Information Offices and Directors of District Offices; Inside SBA, an inhouse newsletter, and The News Digest, a clipping service. Information about SBA programs is also issued by this office. About 100 publications are produced inhouse; none are contracted out.

A monthly video show is produced on BusNet called the Small Business Report, covering a theme of national scope such as exporting. Videos are also produced to be used for inhouse training programs.

A staff of three in the Publications Office answers telephone inquiries. Approximately 100 calls are received each day. However, most of their time is spent responding to written requests.

No official marketing of publications is done.

MANAGEMENT ASSISTANCE

Mission and Scope. The Office of Management Assistance conducts the largest program of information dissemination of the SBA Central Office. Most SBA publications originate from this office, as well as all counselling programs and the authority for training and course development.

Publications. Ten million publications are issued each year. Eighty percent of the publications are pamphlets called management aids, bibliographies, or fact sheets that are available free. About 2 million are flyers, called catalogs, which list publications available free or for a charge. Some training manuals are produced for courses given in the field offices. The remainder of the documents published are booklets of over 20 pages which are sold by the Government Printing Office or the Consumer Information Center to the general public. All SBA publications are free to their clientele.

Free publications are distributed through a contract with the Federal Prison Industries unit called UNICOR at the Ft. Worth Correctional Facility. UNICOR is responsible for the warehousing, handling, and mailing of these publications.

Management Assistance publications cover a wide range of topics of interest to the small business. Most of them are written by persons outside the agency free or under contract. Management Assistance staff is responsible for editing the documents for uniformity and having them published.

Films are also purchased for use in training programs.

No marketing is done because response would overwhelm the funds available to produce publications.

Changes since 1976. The price of SBA publications for sale went up considerably with the 1981 change of administration at GPO.

There were 800 Management Assistance titles in the late 1970's, including some highly technical publications on research and engineering. Now there are 200. Reform 88 inspired substantial budget and staff cuts and an increase in paperwork. The office must produce much paperwork detailing the cost of each publication on an annual basis. All publications must be approved by the SBA Office of Public Communication, which maintains liaison with Office of Management and Budget. There is some disagreement with OPC as to the extent to which they may require modification of documents before approval.

Formerly there were eight or more writer/editors and several film staff. Now there are two writer/editor slots, one of which is filled. One person assigned to other tasks helps out by buying films. The film staff used to contract out for the production of new films.

Staffing changes have completely altered the operation of the office. Formerly the emphasis was on internal production of documents. The one writer/editor cannot even find time to revise old publications or develop new ones. He can only manage contracts for others to write publications. The administrative burden is so great that the office is considering contracting- out for editing as well as writing. However, funds are not available at this time.

Counseling and Training. There is today an almost limitless demand for courses and training sponsored by the SBA. Ten years ago the demand was not as great. The Management Assistance Center maintains control over training by generating guidelines to the local offices where it takes place. Field offices may also agree to cosponsor courses given by community colleges. Cosponsorship allows the college to use SBA course outlines, publications, and limited franking privileges.

Extensive funding has been granted for the establishment of Small Business Development Centers across the country. The SBDC contracts with a university in each state to set up a consortium of universities and Chambers of Commerce to do

counseling. These contracts include a certain amount of research. A clearinghouse will be set up to keep track of the research studies generated under SBDC contracts. A feasibility study of computerization of this clearinghouse is being undertaken.

Counseling is provided in the field offices under the SCORE program, where retired executives volunteer to provide advice. Quick drop-in meetings of less than an hour are not recorded. More extensive meetings of greater than an hour, where there is usually a follow-up visit, are entered in the SBA mainframe computer system. About 250,000 such visits take place each year.

The computer record consists of the business name, location, general type of problem, type of counselor (staff or SCORE), location of the counseling, resolution, minority or veteran status, and whether the case is open or closed. Only the narrative portion of the manual record could contain confidential business information, and that is not entered online.

The communications system was already in existence for the transmission of financial information. Management Assistance uses have been piggybacked on the existing system. District and Regional Offices have dumb terminals for the entry of data into the system. Training statistics are also entered.

SBDC counseling data is being entered by the university responsible for establishing the consortium. Formerly all SBDC data went into a separate regional computer system.

Freedom of Information. Requesters are usually not asked to go through the formal FOI procedures since most requests are for statistical or general information. About six requests are received a day, and one or two will be for statistical information. General information about small business or management assistance activities will be answered by the appropriate staff. Statistical questions are referred to the Planning and Evaluation Branch, which is responsible for issuing quantitative reports. All questions are answered from staff knowledge or reports.

Requests for lists of persons counseled are denied, or those asking are told they must file a formal FOI request.

Extent of Computerization. This office uses Wang word processing equipment. They cannot access the central computer or communicate with the field offices through the Wangs.

FINANCIAL DIVISION, WASHINGTON DISTRICT OFFICE

Mission and Scope. The Financial Divisions of the District Offices of the Small Business Administration are the major focus of information collection activities for the agency. Personal information is collected by these offices as part of the loan application and processing procedure. Except for some loans where the total project cost is greater than $500,000, all loans are processed and approved or denied at the District Office level. Applications for loans for projects exceeding that figure must be approved at the Regional level.

Each action taken on a loan, whether it is approval or denial, must have two signatures. The usual flow of applications is from the clerk to the Chief of the Financial Division, who makes a preliminary analysis of complexity and assigns a loan officer accordingly. After a loan official makes a determination, the Chief reviews the final action. There is an appeal procedure where the denial is reconsidered first at the District level and then at the Regional level.

Information Procedures and Extent of Computerization. Three file systems are presently maintained by this office. A manual system will be dropped shortly. The office has been in the process of converting from the manual system for a year. There is the Loan Assistance Tracking System (LATS), which tracks a loan consideration from application through disbursement. Another system containing the same data is being implemented on a Wang personal computer. Both systems are used to give statistical information and reports and for internal file management.

The Wang system was started because LATS was not able to produce information in the desired formats. Access points in the LATS system are only the name of the business applying for the loan, and the loan number. The PC system theoretically allows for access to any point desired. This system has only been in use for six weeks, and guidelines have not been officially developed. No Automatic Data Processing safeguards are employed in the Wang system, and there are no agency-wide ADP standard operating procedures being applied to its operation at this time. The Division may decide to concentrate on one system once cost effectiveness evaluations are completed. The Washington regional area is piloting increased computer use for the rest of the regions across the country.

While an application is being assigned to a loan official, the office clerk orders credit reports on the applicant and forwards their SBA Form 912, Statement of Personal History, to the Inspector General's Office at SBA Central. This form asks the applicant to list any arrests, convictions, or indictments for any criminal offenses other than minor motor vehicle violations. Applicants on probation or parole must so indicate. A computer check of this information is performed through

the National Crime Information Center (NCIC) system. An attorney who used to work for the Washington District Office stated that an arrest or conviction of a crime is not in and of itself grounds for loan denial. The type of crime is relevant, with applicants having a record of financial crimes at greater risk of having their applications denied. Information obtained from NCIC is simply regarded as one more element in the total picture of the applicant and his or her business, from which the loan officer must make a judgment.

Personal financial information is also collected from applicants on SBA Form 413. The loan application form, SBA Form 4, contains business financial information of a nonconfidential nature. All forms used have clear instructions on the back or face of the document. "Statements Required by Laws and Executive Orders" is the title of a notice given to applicants that explains the laws governing information provided on the application forms. Applicants are asked to acknowledge that they have read the form and authorize the release of information contained in a disaster loan application.

Another document that may be used is SBA Form 641, Request for Counseling. Applicants for direct loans, who must have been turned down for commercial financing, are strongly encouraged to fill out this form and obtain counseling through the Management Assistance Office of the Washington District Office. The counseling request can contain confidential business information in the narrative that delineates the problems encountered by the applicant. (See discussion under Management Assistance.)

The control clerk logs in the name of the business, its location, type of business, amount of loan applied for, and whether it is direct or guaranteed. The applicant's sex and minority status is also entered. This basic information is flushed out later with information generated from the approval process. There are about 60 items in the loan approval document, mostly financial data such as interest rate, that is kept for statistical purposes. Once entered into the system this information can be accessed throughout the District office and is used primarily by program staff for reports and speeches.

Log information is currently entered into each of the three systems. Until October 1984, log forms were batched and entered into LATS by someone in the Office Information Center, the District Office's ADP center. Now the control clerk enters log information directly from the forms at a terminal located in OIC. Soon the office will have its own terminal and when the manual system is dropped data will be entered directly from the case file. Case files will continue to exist

in hard copy.

Once applications are approved, the case file is sent over to the Legal Division, which has authority during closing. Once the loan is disbursed the file is transferred to the Portfolio Management Division (PMD), where loans are managed. No hard copy files are retained by the Financial Division.

Information systems and procedures are generally the same in PMD as in the Financial Division. PMD has a small manual system which provides access by company name and name of borrower. This system will continue to be maintained even after automation is completed. A manual delinquency system will be discontinued. This office uses the Loan Accounting Query System to enter any administrative actions taken on loan files, such as a deferment of payments and recording payments made on loans.

Applications are also processed by the Minority Small Business/Capital Ownership Development Office, for qualification for the subcontracting program of that office. Again, procedures and systems are about the same.

FOI/Privacy—Staff Training. Data is almost never requested from this office under either act. One FOIA request per year is a rough estimate. The Portfolio Management Division might get one request per quarter.

There is no formalized training of FD staff in privacy issues. The office policy is not to release anything but the name of the company, the address, and the amount of the loan received. If any further information is requested, the matter is referred to the District Counsel.

Periodic briefings of PMD staff are conducted by the District Counsel's Office on privacy and freedom of information issues.

Applications are also processed by the Minority Small Business/Capital Ownership Development Office, for qualification for the subcontracting program of that office. Again, procedures and systems are about the same.

LEGAL DIVISION, WASHINGTON DISTRICT OFFICE

Mission and Scope. The legal divisions of the District offices act as agency advisors in the areas of commercial lending and government contracts. They close loans and act as litigators in loan collection actions where SBA is a party. As a collateral duty, the District Counsel is responsible for initial action on Freedom of Information requests.

Freedom of Information Act. The majority of Freedom of Information Act initial

requests at the Washington District Office level are handled by the District Counsel. The legal division in the Washington District Office consists of two attorneys, a paralegal and a temporary attorney. Responsibility for FOIA and the Privacy Act is a collateral duty of the supervising attorney, who handles 60 percent of the requests and delegates the remainder to the other attorneys. Washington District Counsel denied 9 out of 60 FOIA requests in 1983.

Requests come in as referrals from the FOI Officer at the Hearing and Appeals Office, or from the public. Attorneys make up the biggest group of public requesters, with government contractors coming second. Other business entities represent the next largest type of requester, and the remainder (a small percentage) are the general public.

Some requests come by telephone. If the request is for clearly disclosable information, then the information will be supplied. Similarly, requests for impermissible disclosures that can be readily answered will be handled on the telephone. If the attorney must look at the document to determine if it is disclosable, or if the document must be searched for, then the requester will be told to write down his request.

A typical request that is routinely denied over the telephone is for a mailing list of all loans made last year to be used for sales purposes (13 CFR 102.4J prohibits such disclosure). A typical request routinely granted over the telephone is: "Did ABC Co. get a loan and who are its officers?"

Routine written requests include applications of other companies for assistance, to be used as a model by the requesting company; contract specifications; and legal documents creating a security interest such as notes, mortgages and deeds of trust.

When a written request is considered, the attorney must first find the document requested. Most information desired is in the area of lending or contracting activity. A copy of the request will be sent to the supervisor of the division, who is asked to find the file and the person responsible for servicing the file. Eighty percent of the written requests can then be handled by the attorney from the documents. In the remainder of the cases the attorney must discuss the request with the specialist responsible for servicing the file. After the disclosure determination is made, the requester is sent the documents, or the disclosable parts, or the notice of right to appeal. Usually no fees are charged because of the burden of collecting money.

Extent of Automation. Some requests, usually a listing of contract granted, are

filled by printouts done by someone in the pertinent program office. The majority of requests are filled by paper copy.

Two files are maintained manually: a log and a FOIA file. The file contains a complete record of the entire transaction of request and response. The log is a tickler system that contains non-FOIA information as well. Information requests are logged in in chronological order by name of the requester, the staff person to which it is assigned, and a log-out date. There are plans to automate the logging system.

Changes Since 1982. Prior to 1982, there was no logging system and no organized FOI file.

Privacy Issues and Staff Training. The attorney interviewed had never received a request under the Privacy Act. He was not required to identify any systems of records. Other than the Justice Department FOIA training, there is no formalized staff training on privacy issues.

DATA ANALYSIS AND SYNTHESIS

As before, the eight criteria for assessing the impact of technology use on data collection, access to rulemaking and public information distribution were applied to agency information handling practilces. Since technology use is just beginning at SBA, it is difficult to determine any civil liberties implications at this time.

1. **Constituencies Affected.** The constituencies of SBA are primarily small business owners and organizations representing small business. Also affected to a lesser degree are state and local governments and business organizations, as well as the general public. On the whole, information practices and procedures created no negative effects on SBA constituencies .

2. **Public Meetings and Public Comment.** Since the Small Business Adminstration is not a collegial agency, the Sunshine Act does not apply to require the holding of public meetings. While the SBA has an advisory group of business persons called the Small Business Advisory Council, it need not open its meetings to the public because it does not fall within the definition of an advisory committee under the Federal Advisory Committee Act.

3. **Dissemination of Publications.** Information technology has not altered the number or type of publications disseminated by the SBA. However, there has been a decrease in the number and type of educational publications put out by

Management Assistance due to budget and staffing cuts. Formerly, Management Assistance staff would supervise the production of films to be used in training and counseling of entrepreneurs. Now these must be purchased. The total number of educational and technical titles produced by Management Assistance went from 800 in the 1970's to 250. Reform 88 brought the figure down to 200 titles.

In the Central Office, dissemination of written and oral information is carried out by the Offices of Advocacy, Management Assistance and Public Communications. Most dissemination, however, takes place at the field or regional office level.

4. Contracts for Information Dissemination. The majority of the publications issued by Management Assistance are written at no charge by academics or are contracted out. The reduced staff no longer has time to revise old publications and create new ones. Even time for editing papers written by contractors is limited. If funds were available, the editing function would be contracted out also.

Most distribution of documents is carried out inhouse throughout the agency. Management Assistance, the largest disseminator at SBA, does have a contractor, UNICOR, to warehouse, package and distribute free publications. Some Management Assistance booklets can be purchased from GPO or Department of Commerce field offices. Research studies produced by the Office of Advocacy are sold at the National Technical Information Service.

5. Library Closings. There have been no library closings at the SBA. The Small Business Information or Reference Library is providing valuable reference services to agency constituents and the general public, as well as to SBA Central and field offices. There do not seem to be any plans to close the Reference Library. The Law Library, not investigated for this study, is maintained only for use of the legal staff.

6. Marketing. The Small Business Administration does no official marketing of its publications. A Management Assistance staff person stated that their budget would be overwhelmed if they were to actively market.

In the agency's role as the advocate of small business, the Offices of Advocacy and Public Communications market SBA publications and services through press releases, newsletters, research summaries and analyses. When community colleges obtain SBA cosponsorship of their programs and courses, the name of the Small Business Administration is used in the advertising of the courses. SBA publications are used as course materials and students are given copies of SBA catalogs of materials. This could be considered indirect marketing of SBA public information.

7. Personal and Company Information Rights. No infringement of personal or company information rights was documented in any of the SBA information handling practices. The computerized files such as the loan accounting information and the records of counseling, do not contain a great deal of confidential information. Although Social Security number is used as a personal identifier in the loan files, computer runs are not performed on that field. There was one computer matching program carried out to identify farmers receiving duplicate disaster loans, but there are no plans to repeat that match or to conduct any other matching. National Crime Information Center checks are run on individuals applying for business loans. Unless an NCIC search can be demonstrated to be the sole basis for the denial of a loan, it is doubtful whether the practice of running criminal checks constitutes an infringement of personal rights.

Similarly, the practice of reporting of loans and their payment status to credit agencies under the Debt Collection Act does not at this time appear to equal an infringement of civil liberties. Since the reporting is done pursuant to Federal statute and OMB regulations, either some irregularity in SBA's actions or a defect in the law must first be demonstrated.

Agency procedures, such as the Privacy Act Procedures SOP and the System of Records Index, are in place to ensure the protection of company and individual privacy in the normal manipulation of SBA data bases, manual files, and Freedom of Information Act responses. FOI Office staff is trained at the Department of Justice and elsewhere in privacy issues, and inhouse programs are conducted for staff in other departments.

The SBA response to FOIA requests is principally at the District level and the scope of this study did not permit an examination of more than one district office. If this office is typical, it would appear that requests for information are handled in a timely and conscientious manner.

The Freedom of Information Appeals Office keeps track of FOI requests handled initially at the Central Office, as well as managing appeals. Inquiries necessitating computer runs, even those from field offices not made under FOIA, must all be transmitted through the Director of the Office of Computer Sciences. This step exerts even more administrative control over the flow of information out of SBA. Coordination with the FOI Officer and the Office of General Counsel is also required.

8. Security.

SBA is reportedly unusual in the Federal Government, in that the agency

Program Computer Security Manager is a member of the Inspector General staff. He and the Office of Computer Sciences Security Officer have developed and implemented security practices and procedures for computer and manual files. New guidelines are being developed with the Information Center team for security of the new minicomputer. SOP 90-25, Computer Systems Security, is presently being rewritten to accommodate technological and legal changes.

TOPICS FOR FURTHER RESEARCH

Once SBA's new distributed mini- and microcomputer system has been operational for a sufficient time, it would be worthwhile to re-examine agency practices in the context of personal and company privacy issues.

Two SBA practices that merit further attention are the reporting of loans to credit agencies and the NCIC checks on loan applicants. The controversial reporting program under the Debt Collection Act, if and when it moves into the third phase of reporting consumer loans, should be looked at in the context of possible violations of financial privacy. Very small business concerns (five or less partners) also come under the jurisdiction of the Right to Financial Privacy Act (12 U.S.C. 3401 et seq., 1978) and therefore SBA's present reporting of commercial loans made to businesses of that size should be examined as well. Subsumed within the general issue of financial privacy are the concerns of access, integrity and accuracy. Any information transmitted to credit agencies and possibly downloaded to credit bureaus must be accurate and protected from unauthorized access and manipulation.

Major problems with the record quality of NCIC files have been asserted. One major problem cited was inaccurate disposition, charging or sentencing information (OTA, October 1982, p. 91). Severe policy implications could arise if an SBA loan were denied on the basis of inaccurate information contained in NCIC files. A study of SBA reliance on NCIC checks in the loan decision making process, and the resultant denials, would be worthwhile.

4.7 VETERANS ADMINISTRATION

INTRODUCTION

The Veterans Administration was established as an independent agency by Executive Order 5398, July 21, 1930, in accordance with 46 Stat. 1016 (1930). The 1930 statutes were modified and expanded in the present laws governing the VA, 38 U.S.C. 101-5228.

The VA administers an extensive program of benefits for veterans and their dependents or survivors, including compensation for death or disability, pensions based on financial need, insurance, education and rehabilitation, home loan guaranty, burial, and comprehensive medical services.

This agency is divided into three principal departments: Medicine and Surgery, Veterans Benefits and Memorial Affairs. Only the first two are within the scope of this study. These departments at the Central Office level set policy and define procedures for VA operation at the field level. The Department of Medicine and Surgery (DM&S) supports nursing homes, clinics and 172 medical centers. VA Regional Offices are field stations which grant benefits and services to veterans and their dependents, or other beneficiaries. Applications for loans and other benefits are taken and acted upon at the regional level. Therefore, most agency information collection and dissemination is decentralized. Because of the time constraints of this study, it was not possible to research information practices in the field.

Within the Central Office, directorates and offices have been set up to further the mission of the Veterans Administration. Since the appointment of the present Administrator, the policy has been to consider all administrative offices as support for the functions of the three departments.

The VA has used computerized data bases for some time. The operation of such a large effort of veteran support necessitates the maintenance of many files. However, like the other agencies profiled, the VA is just beginning to automate office functions through the use of microcomputers and word processors. Microcomputer/mainframe linkages are just being developed and implemented. In these areas, the impact of agency technology use on civil liberties is yet to be assessed.

Because the VA administers monetary programs of such magnitude, overpayments and delinquencies can represent a significant drain on program

resources. Consequently, the VA has initiated an extensive program of computer matching to identify ineligible benefit recipients and those with delinquent accounts. While computer matching in general represents a use of personal/confidential information that merits evaluation for civil liberties impact, the VA appears to be conducting its matching programs in a manner in accordance with the law.

This profile will describe the organizational units within the Central Office that are the primary loci of information collection and use, dissemination, and access to rulemaking. A number of support offices that report to the Associate Deputy for Information Resources Management were examined, including the Office of Data Management and Telecommunications and the Office of Information Management and Statistics, and their respective subdivisions. The profile of the Office of the Inspector General contains all the data obtained on agency computer matching. Two agency program departments, the Departments of Medicine and Surgery and Veterans Benefits, were then researched to assess their involvement in the dissemination of public information. Departmental data use is discussed within the section describing the Office of Data Management and Telecommunications.

Following the description of VA information-handling practices, civil liberties impact will be discussed in the Data Analysis and Synthesis section and questions for future research raised.

ASSOCIATE DEPUTY ADMINISTRATOR FOR INFORMATION RESOURCES MANAGEMENT

Mission and Scope. The Associate Deputy Administrator (ADA) for Information Resources Management is the senior agency official for purposes of the implementation of the Paperwork Reduction Act. The IRM activities supervised by the ADA include office automation; ADP, telecommunications, and acquisition of those systems; agency reports; paperwork management and VA regulations. This office was described as the focus for management within the agency.

The ADA monitors VA compliance with the Federal Managers' Financial Integrity Act, OMB Circular A-123 and Circular A-109, Procurement of Major Systems. This office is responsible for the vulnerability assessment required by A-123. The assessment is performed without regard to the ADP considerations central to an A-71 risk assessment.

Reporting to the ADA are the Office of Information Management and Statistics, the Office of Data Management and Telecommunications, and the

Management Control Staff.

Office of Data Management and Telecommunications

Mission and Scope. The Office of Data Management and Telecommunications (ODM&T) is one of the major operating elements of the VA. Approximately 2,000 people are employed in this office. Its mission is to provide ADP and telecommunications support to all Veterans Administration offices and medical centers nationwide. The Office operates five Data Processing Centers throughout the country, and a national VA Data Transmission System (VADATS). Most of the ADP systems development and ongoing ADP production is accomplished at the regional Data Processing Centers. The Director of ODM&T serves as the principal advisor to the Associate Deputy Administrator for Information Resources Management and to the Administrator of VA on ADP and telecommunications policy, practices, technology, office automation and information resources management.

Major Automated Systems. The publication "Active ADP Systems/Applications" lists 141 active automated systems at the VA as of January, 1984. The major systems serve the largest VA users, the Department of Veterans Benefits (DVB) and the Department of Medicine and Surgery (DM&S), who in turn provide direct benefits and services. Possibly the most up-to-date system is TARGET, a non-acronym for several files containing pension, compensation, and education benefits information. Also referred to as CP&E, the system provides online support of DVB regional offices in processing claims and producing payments.

Other DVB files which pertain to this study are the Insurance System (INS); several loan accounting systems; BIRLS, the Beneficiary Identification & Records Locator Subsystem; and CARS, the Centralized Accounts Receivable System, which encompasses the entire DVB debt collection process and tracks overpayments made by CP&E. BIRLS serves as the repository for veterans service records and as the locator for folders containing other information on the veteran. BIRLS is identified by name of serviceman, but the record contains mostly file numbers and locations rather than personal information. CARS and BIRLS are online systems.

In the Fiscal Year ending in September 1983, ODM&T complied with the VA's debt collection law, P.L. 96-466, by modifying CARS and CP&E to assess interest and administrative charges against education overpayments. CARS generated two mass mailings to one million recipients of overpayments. The VA will be communicating all delinquencies (delinquent loans and benefit overpayments) to credit reporting agencies under the authority of the Debt Collection Act. Reporting is expected to take place in early 1986. No earlier date is possible

because of technical problems. All accounts receivable are maintained in St. Paul, Minnesota, yet all policies and procedures must be established at the Central Office in Washington, D.C. The format of VA files is at present different from the format acceptable to Dun & Bradstreet.

Within DM&S, the principal system containing personal information is the PTF, or Patient Treatment File. A record is maintained of all care given to each patient admitted to a VA facility or to a non-VA facility at VA expense.
The file is kept primarily for statistical reasons: it contains personal, demographic and clinical data. The system is listed as exempt from disclosure under the Privacy Act because personal identifiers are used. Presently, medical personnel in the field use the teletype to input data but they cannot access the file to generate any information. Access to the paper or fiche output of the system primarily occurs at the Central level.

Other data bases will be discussed below in the pertinent sections.

Directorate for Telecommunications

Mission and Scope. This directorate has primary responsibility for VADATS, the VA Data Transmission System. VADATS is a message store and forward system used for transmitting messages and financial, payroll, supply and personnel data between the field offices and hospitals and the Central Office. VADATSwas originally ARS, an old General Services Adminstration store and forward system. Responsibility for the system was transferred to VA in January 1984.

Security for VADATS is high, partly because it is tied into the Department of Defense system. Further security is provided by the use of access codes and Department-level security procedures, and because the information is transmitted by means of a packet switching network.

Directorate for ADP Policy and Operations Management

Mission and Scope. This directorate is the focal point within ODM&T for Computer Security and other issues of ADP policy and data management.

The policies developed by this office for the VA focus on three technological strategies in the areas of system design and integration management, telecommunications, and integrated computing support services. The strategic initiatives in these areas were described as follows: data should be integrated, or available to whomever has a "need to know"; data communications must be regarded as a utility—there will not be multiple networks; and computer services will be integrated—the skills and tools of the end user will be taken into consideration, but

always in the context of a unified ADP system.

These policies are explained in a statement issued November 15, 1984, by this directorate (attached in Appendix C entitled "Automation of Administrative Processes." This document identifies an agency-wide focus on data and technology sharing. Shared data will be used to create new data bases that will serve information need vertically within a department and horizontally to other departments and staff offices. The communications network will be gradually implemented by purchasing new equipment with communicating capabilities and replacing old equipment as it becomes obsolete. New and emerging technologies are to be employed both for centralized computer systems and for decentralized equipment. The Data Processing Centers in the regions will shortly have online access and responsive capacity.

Security. The Associate Director for ADP Policy and Operations Management is the ADP Security Officer for the Agency. Within each department of the VA there is a departmental Security Officer and a Systems Security Officer. The Systems Security Officer deals with the privacy and integrity of departmental data bases. At the regional level, each regional office or station has its own security officer. Access to departmental data bases such as the DVB loan files is not allowed without some security clearance and the possession of a Terminal Access Card, as well as knowledge of the necessary passwords. The DVB computerized files were described as a transaction-driven system. Officials in the field may access Central Office DVB data bases to read and update the files, but integrity is maintained by the requirement of two "signatures": the person who establishes a claim cannot also authorize payment. Internal system controls prevent any unauthorized changes.

Staff persons is each department are constantly reminded of security concerns. Three security officers of DVB audit the stations on a regular basis. Daily reports are generated by the station systems which are used by the Central Office for monitoring of file use.

A Steering Committee was set up last year to promote an awareness of security issues. The Committee consists of ADP Security Officers for each office and department. A draft of an ADP Security Handbook for use by the recipients of office automation was developed by the Committee. It will be completed by a contractor in three months.

Three surface security issues for non-ADP staff were identified: personal security clearances; physical and logical security for information; and developing a constant awareness of security. Logical security was defined as the organization of

data so that it may be protected; software controls must be developed to prevent unauthorized information flow between systems.

A new security staff is being developed to cover data management and security for ODM&T. The head of this staff will also become the Agency Security Officer. A meeting will shortly be set up between the Inspector General's Office, the Office of the General Counsel, ODM&T, and the Office of Information Management and Statistics to discuss data sensitivity. The emphasis will be on the privacy and integrity of the financial and payment systems.

VA Manual MP-6, "Automatic Data Processing," Part I, Policy, was recently revised. The chapter on security applies to all systems involved in information processing, both mainframe and microcomputers. An information sensitivity system is set out as follows in descending order of sensitivity: 1) Critical-sensitive (Top Secret classification; grave effect on VA mission; involved in funds distribution or controlled substances applications); 2) Noncritical-sensitive (Secret or Confidential classification; serious effect on VA mission; proprietary or privileged information; protected under the Privacy Act; pertaining to an individual identifiable by name, Social Security number or other unique identifier; or derived from Inspector General activities) 3) Nonsensitive (no special protections required). Each level of sensitivity is to have physical and logical controls in accordance with VA policy. Each facility has its own security officer who conducts the risk assessment and establishes the security controls for sensitive information. Guidelines for the application of policies cited in VA Manual MP-6 to microcomputers are contained in Circular 00-84-26, "Office Computers."

Information Technology Center

Mission and Scope. The VA Information Technology Center (ITC) within the Office of Data Management and Telecommunications functions in three areas: basic training, technological support, and technology evaluation. According to the ITC brochure, the mission of the center is to increase awareness of how computing technology can enhance productivity; to promote greater self-sufficiency of noncomputer personnel in the evaluation and application of personal computing; and to facilitate VA-wide information and resource sharing. The Center has been open one year, and is available to managers, professionals, administrative personnel, and computer specialists.

A wide range of training classes is provided, from basic computer literacy to advanced software use. When an office needs technological support, ITC staff will put together a hardware and software configuration based on user needs. The

office must initiate the procurement process. Once the equipment arrives, ITC will perform diagnostic tests and set up training for the office staff. The technology evaluation function of the Center is an ongoing process: new technologies are installed at ITC and researched by that staff. Current systems under evaluation are the AT&T 3B2 Super Micro and the PC Net local area network.

The Information Technology Center expects to be directly involved in the installation and operation of a network system. ITC will provide the shared hardware, including a laser graphics printer, and a public disk containing management information such as budgeting reports, staffing status, and workload tracking. All these documents are currently reproduced and circulated in hard copy.

Information on microcomputers is made available to VA staff not only through the training and courses, but in publications such as the ITC Update, a monthly newsletter. A library of documentation, periodicals, and monographs on personal computing is maintained. The topic of data security and privacy is an important issue in ITC publications and training.

The Center also performs other functions relegated to them because of the equipment ITC maintains. Electronic mail is provided for some offices that do not have equipment that can communicate with the regions. Medical documents can be sent from an office Lanier word processor to a personal computer in the ITC, and from there transmitted to a regional office or medical center.

Technological Changes for ODM&T. A large open-ended contract was just signed with a vendor to supply VA with office automation equipment. The first to be automated will be ODM&T and the Office of the Controller. Most data flow within these offices is internal, but they, along with all other offices, will be provided equipment that will interface with VADATS. The personal computers and word processors will be used for electronic mail, correspondence, and management reports. Most intra-agency communication is between peer level organizations. Agency-wide transmissions are usually messages from the Administrator, announcements, and policy documents. The problem of maintaining a "signature trail" is not an immediately foreseeable issue, according to one official interviewed. The Administrator's Office serves as the control point for all communications. All documents transmitted electronically are assigned code and validation numbers.

ADP systems will be frequently re-evaluated to incorporate new technological improvements. More effective delivery of services and improved management information are the expected results of the planned automation and redesign of

present systems. There will be an increased emphasis on user access of existing automated applications systems.

VADATS will be upgraded to provide the real time communication necessary to support interactive data processing throughout the VA, as well as improved message store and forward service for administrative message traffic and batch processing.

Office of Information Management and Statistics

Mission and Scope. Parallel to the Office of Data Management and Telecommunications, as one of two offices under the ADA for Information Resources Management, is the Office of Information Management and Statistics. Although ODM&T is considerably larger, both offices report to the ADA and complement each other in making up the total picture of information resources management. The Office of Information Management and Statistics (OIM&S), formerly the Office of Reports and Statistics, was renamed in April of 1984 and given new responsibility for paperwork and records management. Much of the public information disseminated by the Veterans Administration is released from this office. Its information function is largely based on the acquisition, analysis, and dissemination of statistical information about veterans and programs of the VA. Economists, computer specialists, and management analysts are the professional staff of this office. They are broken into three divisions: Statistical Research and Analysis Service, Reporting Policy and Review Service, and Paperwork Management and Regulations Service.

The Reporting Policy and Review staff formulate standards for operating the VA's integrated reporting system, and review and control all proposals to obtain VA, interagency, or public-use reports. This service also coordinates improved reports management, as required by the Paperwork Reduction Act, and works with ADP systems in the preparation of management information and agency-level reports.

Paperwork Management and Regulations staff recommend general policies for the creation, maintenance, and disposition of VA records. FOIA and the Privacy Act are administered under this Service.

The Statistical Research and Analysis Service provides estimates and projections of the veteran population and its needs and resources. The Veteran Population Model was derived from 1980 Census data on an aggregate basis. By applying this model, the characteristics and size of the veteran population can be predicted up to the year 2050, assuming another major war does not occur. Such predictions are used by program managers for planning purposes.

Using data from different VA reporting systems, the professional staff analyzes

mortality levels, patient stay, and results of health care treatment. Special and recurring studies are conducted to measure the impact of specific benefit programs. Statistics about the veteran population as a whole must be collected by the Service: all other VA data collection is done as a part of the operation of departments that administer various benefit programs, and the information collected is specifically geared to the individual department. Statistics used and collected by this Service are generally nonindividual demographics.

Publications. Nineteen recurring reports are issued by OIM&S, with titles such as "Disability & Death Pension Data" and "VA Trend Data." In the April 1984 catalog of statistical publications, nine non-recurring reports and eight non-recurring statistical briefs are listed.

Printing. Until October 1984, the Veterans Administration operated its own printing plant. Now it must rely on GPO and contractors selected by GPO. Once a document is written by OIM&S it is sent to the Publications Service within the Office of Administration for typesetting or reproduction by direct image. After typesetting, reports are sent out for printing.

Marketing. A mailing list is maintained of persons wishing to receive recurring reports. The list is sent to Publications Service for actual mailing. Anyone can receive VA statistical publications. No formalized marketing takes place. However, staff putting together a study are asked to consider the intended audience of the publication. Usually it is the veteran public, or veterans' groups, but it may be the entire Congress, VA authorizing committees, oversight committees, or Directors of Veterans Affairs in the states. Publications intended for any of the latter are often directly mailed to them. Otherwise, a copy of the latest catalog listing publications will be sent.

Staff present papers at professional societies and publish articles in American Demographics as a means of promoting national awareness of VA statistical studies and publications.

Other Dissemination of Public Information. The Service receives several thousand telephone calls a year from Congress, OMB, GAO, and the press requesting statistical information. Most press calls are handled by the Office of Public Affairs.

Privacy Impact. Inasmuch as the data used and collected by the Statistical Research and Analysis Service is not descriptive of individuals, there is no impact on privacy and confidentiality issues by this office's statistical operations. The only file maintained by OIM&S with possible privacy implications is RONA, the

Release of Names and Addresses. Under the Veteran's Administration legislation, the Administrator is allowed to release information from the education, compensation/pension and discharge systems to Congress and nonprofit organizations if the stated purpose is to notify veterans of their benefits entitlement. Only names and addresses may be released, and use of the system is monitored to prevent abuse.

Changes since 1976. There have been no changes in operations or publications due to budget cuts or reductions in force, since these have not occurred at the Veterans Administration. Agency-wide changes in the application of technology are occurring in the office automation process, but any impact on the civil liberties areas under investigation is yet to be observed. The installation of the current Administrator of the VA resulted in a change in operational structure and theory. Since his appointment, the operations staff function as support to the three departments, not just to the Administrator or to the agency as a whole. The functioning of the OIM&S has been altered since the information resources duties were added on.

Paperwork Management and Regulations Service

Freedom of Information Act. The Director of the Paperwork Management & Regulations Service within OIM&S serves as the Freedom of Information/Privacy Act Coordinator for the Agency. He is responsible for agency-wide policy in those areas. Most requests for information are received at the regional or departmental level. If letters come in to the VA addressed to the Coordinator or to the FOI Officer, this office quickly reviews them to determine the appropriate department or office. In the infrequent instance where more than one department is involved, the Coordinator will provide the Agency response. Where a request appears to involve a legal issue, it will be forwarded to the Office of the General Counsel. The response will then go out under the name of the Coordinator, because the OGC serves in an appellate capacity for contested FOIA cases.

The Coordinator's office keeps a copy of the request and the forwarding letter chronologically. There is no tracking system because the number of letters forwarded is small. FOIA requests made directly to the department or other division involved may be tracked because of the larger volume.

Requests for information seen by this office are usually single-party requests for data from insurance, medical or claim files. Many people believe they must ask for information under FOIA, when the operative statute is really the Privacy Act. Although FOIA mandates a 10-day time in which to respond to requests, whether

the information is available or not, VA policy is to provide the information within 10 days, as well as the response letter. The general Agency policy is to disclose whenever possible. The 1983 FOIA report lists 1,382 initial denials of requests. There is no way to determine the amount of requests made. Fees are charged for duplication of materials and searches.

Privacy Act. MP-1, Part II, Chapter 21, "Access to VA Systems of Records under the Privacy Act," provides internal procedures for dealing with Privacy Act requests. The response time for Privacy Act requests is also 10 days at the VA.

The annual report for the calendar year 1983 shows 53 nonexempt and 4 exempt systems. Requests numbering 44,867 for access to systems of records were shown; by OMB's direction that figure only includes requests that cited the Privacy Act. According to a staff person of this office, if actual requests for privacy-type information not citing the act were included, the figure would be several million.

The Veterans Administration legislation, Title 38, requires the confidentiality of veterans' information in addition to the Privacy Act. Section 3301, Confidential Nature of Claims, only allows the release of information under certain situations (see discussion under RONA above). Section 4132 keeps confidential the medical records of persons undergoing treatment for alcohol and drug abuse and sickle-cell anemia. Two years before the enactment of the Debt Collection Act, Section 3301 was amended to allow the reporting of information to consumer debt reporting agencies. Because of this additional authority, the VA has not published debt reporting activies as new routine uses of systems of records.

The Records Management Division within the Paperwork Management & Regulations Service put the most recent Federal Register compilation of routine uses of Privacy Act systems online. The Federal Register compilation has been out-of-date. Now that the VA portion is online, managers for the record systems will be able to access the data base and keep it current. The data base was put on an IBM 4331 purchased for the use of the Paperwork Management Service. The system will be operational next month.

Records Management. The IBM will also be used for an automated file of Record Control Schedules. These schedules list the records system, whether manual or automated, and the retention period that was approved by the National Archivist. The Records Management Division is working with ODM&T in the design of this system. It will be used as a tool to conform Privacy Act retention periods with approved retention periods. A major part of Privacy Act compliance, as well as good records management, is the identification and appraisal of file systems. At

the VA, good control is exerted over the major automated files—all of the principal systems have been identified and appraised. According to a Records Management staff person, the control over records on smaller machines, particularly in the field, is not asgreat.

There is a dispute in the field of records management as to whether the automated file or the hard copy should be considered the record copy for Archives purposes. One theory holds that where a hard copy exists, the computer file must be considered the working copy, and the paper file deemed the official record. Under that theory, a computer data base can only be an official record copy when no paper copy exists. At the VA, the Patient Treatment File and the hard copy records together are considered to be one system of records for Privacy Act purposes. Formerly, agencies were forced to get approval from the Archivist before paper copies of microfilmed records could be destroyed. New policy allows this decision to be made within the agency. There is some thought that a similar policy should be instituted for records maintained electronically and on paper.

Rulemaking. A Directives Management Divison staff person stated that the printed copy of the Code of Federal Regulations is six months to one year out-of-date by the time it is available to the Veterans Administration. A pilot program was therefore developed by this division to put all VA regulations online on the IBM 4331. New rules and regulations promulgated by the VA will be input to ARMIRS, the Automated Regulations Information Management and Retrieval System, the same day that they are sent to the Federal Register in final form. ARMIRS is to be used only at the Central Office, by terminals throughout the agency. There is no public or field access planned. ARMIRS will be operational in January 1985.

OFFICE OF THE INSPECTOR GENERAL

Mission and Scope. The Inspector General directs an independent organization mandated by the Inspector General Act to audit VA operations and programs. This office investigates Agency activities and recommends policies to promote economy and efficiency, and to detect and prevent fraud, waste and abuse.

Office of Auditing. The Office of Auditing, headed by the Assistant Inspector General for Auditing, performs audits in the areas of: 1) finance and compliance; 2) economy and efficiency; and 3) program results.

Computer Matching. Matching is conducted by computer between VA files and those of other agencies, and between different VA files. The largest matching program

with which VA has been involved was the President's Commission on Integrity and Efficiency project to match the names of persons receiving income-determinant government assistance against the wage files maintained by OMB, TVA, and in some cases DOD. Six Federal agencies participated: VA, HHS, Labor, Education, Agriculture and HUD. The PCIE project, entitled "Federal Employees Receiving Government Assistance," was undertaken to identify Federal personnel who were inappropriately receiving Federal benefits, or who were delinquent on Federal loans.

Four VA benefit programs were selected for review: compensation based on unemployability; pension and other income based payments; nonservice-connected medical care; and beneficiary accounts receivable. The pertinent DVB and DM&S files were matched against Federal personnel earnings records to identify individuals whose income exceeded threshold requirement levels. The VA Centralized Accounts Receivable System (CARS) was reviewed to isolate Federal employees with delinquent debts to the VA. Raw hits were subsequently refined and screened by computer. After final screening, the cases were referred to the appropriate department for verification.

In the verification process, regional offices send letters advising persons that computer screening has indicated an apparent discrepancy in their records. They are given 60 days to dispute the finding. Cases apparently involving fraudulent income statements and applications are referred to the Inspector General for development. The collection process is initiated for delinquent loans and overpayments.

Results of the PCIE Interagency Audit Project are published in Final Report: Federal Employees Receiving Government Assistance, Veterans Administration Inspector General, September 16, 1983. The interagency project was completed, but computer matching continues to be used as an audit tool at the Veterans Administration.

The VA has found computer matching techniques to be effective for detecting and preventing improper benefit payments. As a result of matching audits, DVB management is able to identify instances of fraud, processing errors, and system changes needed to prevent recurrences. The Office of the Inspector General has developed a model for computer matches based on OMB's "Revised Supplemental Guidance for Conducting Matching Programs," May 14, 1982, 47 FR 97, p. 21656.

The Privacy Act report submitted by the VA for the calendar year 1983 lists six matching projects. This figure includes the four initiated as a part of the PCIE project and two new audits. One limited match involved under 7,000 records (out

of a potential 27,000 record base) of persons who might be receiving both income-determinant pensions and Social Security annuities. Pensions, unemployability compensation, and death benefit files of the VA were matched against Social Security Administration annuity files in both name and Social Security number. Raw hits were sent to regional offices for verification. Interim reports indicate no major discrepancies. Income levels reflected in VA files have been found to be inaccurate, but still within prescribed limits once the inaccuracies were corrected. A final report is expected in February 1985. The same VA compensation and pension files will be matched against Railroad Retirement Benefits and Black Lung Benefits files from the Department of Labor in a new project starting March 1985.

The second matching project cited in the Privacy Act report involves wage files maintained by individual states for administering State unemployment insurance programs. The State files are matched against VA compensation and pension records to identify improper payments. The compensation match indicated that regional office information gathering and verification procedures were in need of strengthening. The October 1, 1983, to March 31, 1984, Semiannual Report of the VA Inspector General indicates some disagreement by the Department of Veterans Benefits with the recommendations made by the IG. Internal Audit Report 4AB-B01-050 lists the findings of this matching project.

The pension file match against state wage files is discussed in Audit Report 4AB-B02-045. Only the files of Georgia and Florida were used in the initial match. Substantial overpayments were found. Matching against wage files of cooperating states continues. DVB has proposed legislation to permit access to certain Internal Revenue Service files to verify beneficiary-supplied information collected in applications for income-dependent benefits.

The General Accounting Office in the Philadelphia region performed a multiple correlation computer match of state wage and other data with VA income records for pension beneficiaries. Cases amounting to 444 of apparently erroneous income reporting were found. (Semiannual Report of the Inspector General, April 1, 1983 to September 30, 1983) GAO and VA pension match results are being used in an ongoing project of the IG to forecast the incidence of fraud within segments of the pension system. They have attempted to use the computer data to create a profile, or identify common denominators, of persons likely to fraudulently claim pension benefits. A staff person in the Office of the Inspector General stated that profile attempts had been fruitless: there do not appear to be any common denominators of pension abusers.

The PCIE project has had other follow-ups using VA files. Computer matching techniques were used to identify Federal employees improperly receiving waivers of their VA insurance premium payments (Audit Report 4AB-B12-038). VA data on defaulted education loans was used in an effort by the Department of Education which resulted from the PCIE matches. Federal employees and annuitants who had defaulted on education loans were located (Audit Report 4AB-B05-031). DVB is now receiving the government employees and retirees data base from OMB on a recurring basis. See Audit Report 3AB-B01-123 for results of a review of civil service annuitants receiving income-determinant benefits from VA.

By matching the VA Master Record File with Federal and state employment records, employed individuals who had been rated totally unable to work because of mental disorders were identified in a 1984 audit (Audit Report 4AB-B01-090).

DEPARTMENT OF MEDICINE AND SURGERY

Mission and Scope. The Department of Medicine and Surgery (DM&S) has a three-part mission: patient care, medical research, and education. A fourth function is to serve as contingency backup to the Department of Defense in emergency situations.

Library Division

Mission and Scope. Although the Library Division is organizationally a part of DM&S, it serves as the technical library for the entire Veterans Administration nationwide. The Library Division was created in part to fulfill the educational mission of DM&S—the directorate of Academic Affairs of DM&S operates a Continuing Education Division, which in turn supervises the library. Besides serving the Central Office, the Washington D.C. Regional Office and the general public, the Library provides cataloguing, procurement, and other services to 175 libraries in the VA Library Network (VALNET). Because of its location within the Central Office, the Library Division is referred to as the VACO Library. Most public use of the facilities is by Washington, D.C. law firms who need medical information.

The VACO Library provides supplementary reference service to VALNET. VALNET libraries support the entire VA health care system. The network is broken down into seven Regional Medical Education Center regions. Through these regional libraries, the Central Office provides funding for Dialog access and electronic mail services. Within the further network division into 28 Medical Districts, libraries share journal acquisitions and ILL responsibilities. The Central Office Library

maintains policy and planning control over the operations of VALNET.

Both medical and general collections are maintained at the VACO Library. There are 13,000 monograph and 810 journal titles. Special collections on Aging, Health Care, Herbicides, Military History, and Veterans have been compiled. Reference services, including on-line searching and individually-tailored information updates (SDIs) are provided to staff members. Public users are assisted in using the collection but are not provided automated services. Public business is not solicited. Extensive bibliographies on commonly-requested subjects have been prepared.

An Audiovisual Program Specialist within the VACO Library Division coordinates the development and production of educational materials within DM&S. After an audiovisual program is purchased or produced, it is made available throughout the VA by the VALNET AV Software Delivery System. Materials are distributed at one of four delivery levels, based on cost and demand. At this time the AV catalog does not contain the whole file and it is not available to the public. Once the file is complete and up-to-date, public access may be considered.

Library Closings and Contracting. There has been no attempt to close the Library Division at the Central Office. Such a move would appear highly unlikely considering the lack of Agency budget cuts and the statutory mandate to DM&S to provide educational services. The VACO Library does, however, have a small staff: 8 professional and 2 clerical employees, assisted by 11 part-time undergraduate students. The small number of employees and the extensive management duties performed by each staff person for the Central Library and for VALNET libraries translate into a need to contract out any large-scale projects that involve technical processing, or require technical advice.

Technology. The VACO Library keeps an IBM XT for annual statistics. The first file was put up solely to generate a report on audiovisual production required by OMB. All library functions will shortly be automated: acquisitions, circulation, cataloging and others. In a few months a contractor will start keying in the data.

Publications Management Staff

Mission and Scope. Within the DM&S Communications and Inquiries Division, the Publications Management Staff exerts some control over publications issued by the various medical services of the Veterans Administration. Publications written by this office are exclusively administrative. The Publications Management Staff (here called PMS) reviews the pamphlets and brochures produced by the services, and arranges for the printing and processing. The Research, Nursing and Geriatrics Services issue most of the 25 to 30 publications of DM&S. Most publications

summarize the research and activities of the issuing service.

Dissemination. A percentage of the publications, usually those that are expected to have the widest appeal, are numbered and sent to the Depot for distribution to persons who request them. Other, unnumbered pamphlets must be distributed by the service itself. Each service maintains a mailing list for initial distribution, usually to Medical Centers and regional offices. There is no active marketing to the general public.

Funding Cuts. In the 1984 Fiscal Year, DM&S was required to cut its publication of these documents, considered public relations materials, by 25 percent. The reduction was equally shared between the publishing services.

Research Studies. Research studies were formerly printed in patient printing plants operated under the auspices of Rehabilitative Medicine. These plants are being phased out now. There is currently some concern that the VA is not getting appropriate credit in journal articles for the results of research studies partially financed by VA. Many researchers have a dual appointment by a medical school and the VA. Articles may be published under the university sponsor's name to avoid the necessity of complying with VA publication requirements. Researchers are not required to send a copy of an article to the Library Division, so monitoring of research output cannot take place that way. Other divisions attempt to keep track of research published, but funds and staffing do not permit complete monitoring. The Program Analysis and Development Office is investigating the problem of dual appointment publishing. It is too early to tell the extent of that problem, or if the closing of patient printing plants will result in any significant reduction in the public dissemination of information derived from research studies.

OFFICE OF PUBLIC AND CONSUMER AFFAIRS

Mission and Scope. The Office of Public and Consumer Affairs supports the VA mission in the areas of public information and consumer relations. The Office of Public and Consumer Affairs (OPCA) in the Central Office directs the dissemination of information on benefits and services to veterans, their beneficiaries and the public. VA programs are actively promoted to the media.

Advisory Committees. The Veterans Administration supports some 30 advisory committees in different issue areas, such as Prisoners of War. The Consumer Affairs staff within OPCA prepares Sunshine Act notices for the Federal Register of advisory committee meetings. Copies of advisory committee reports are made

available for public use by the Consumer Affairs division. Since advisory committee operations are considered an important part of policymaking by the Veterans Administration, a handbook was recently drawn up to regulate the management of committee records and procedures. Advisory committee activity increases as the VA becomes aware of more issues that must be addressed. For instance, the Advisory Committee on Women Veterans was established recently.

Dissemination of Information. The Consumer Affairs staff also serves as a conduit for complaints from veterans who feel they have been unfairly disqualified from various benefits. The mediation of complaints is a part of consumer relations, and the staff use the opportunity to better explain the benefits programs.

OPCA staff apply the following criteria to determine whether information should be released to the press: 1) How will it help the veteran?; 2) How will it help the VA serve the veteran?; and 3) Is the public interested? Information on benefits and programs are released to all media, including small town weekly papers.

Much staff time is spent answering inquiries from the press. Many questions also come from attorneys and the general public. About 100 telephone queries are received each day, 95 percent of which are from the press, other VA departments, and Government agencies. Office policy is to answer questions on the telephone if the staff person possesses complete knowledge of the information needed. If a more detailed response is necessary, the caller will be referred to the appropriate program area or to a counselor. OPCA will not provide counseling on benefits.

Publications. OPCA collects assessment data to be compiled in a briefing book for the use of the Administrator and program managers on various issues confronting the VA. This office also has a review function over public outreach documents of the Department of Veterans Benefits: pamphlets that explain benefits and standardized letters to veterans. An inhouse newsletter is published, the VAnguard, and its video version, the VA Video Digest. The Video Digest is being dropped because it has not been found to be useful.

An annual compendium of veterans' and dependents' benefits is the primary publication of this office. Ad hoc pamphlets and posters are produced for special events several times a year. The Agent Orange Review, a newsletter detailing scientific research on herbicides, is published and distributed to veterans on the Agent Orange Registry, field offices, and other subscribers. A pamphlet on radiation effects has also been completed.

Access to Rulemaking. The Consumer Affairs staff provides the means within the agency for publication of proposed rulemaking in the Federal Register. However,

comments are always received by the program officials directly involved with the proposed rule. Within the limited scope of this profile, it was not possible to survey all program officials to assess the potential use of new information technologies for public comment.

Technology. Communicating word processors have been installed for use by the writers. Planned uses for electronic mail will include public relations distribution to the press and to field offices, and electronic response to press inquiries. Distribution to the field offices will be by electronic mail, not only for the speed and convenience but because some statements in press releases have been found to be more effective when attributed to a regional administrator than to an official of the Central Office. The word processors will also be used to keep records and generate reports on topics of media interest.

Changes since 1981. The Consumer Affairs Office was originally a separate unit. Approximately two and one-half years ago it was merged with the News Service. Although there are still separate staff persons who concentrate in each area, the union of Consumer Affairs and News Service has resulted in a more thorough awareness of both issue areas. Public relations efforts now acquaint constituents with the limitations of benefits.

DEPARTMENT OF VETERANS' BENEFITS

Mission and Scope. The Department of Veterans Benefits is responsible for administering the following financial assistance programs: veterans compensation, veterans pension, survivors' benefits, burial benefits, educational assistance, home loan benefits, and insurance coverage.

Veterans' Assistance Service

This office provides an information and outreach service to potential beneficiaries of all VA benefits. A pamphlet is produced entitled "A Summary of Veterans Benefits." A toll-free number is made available which enables anyone to call their regional office to receive assistance in filing claims or to obtain general information about the VA. This office supervises the VADS (Veterans Assistance Discharge System) program operated by the Austin, Texas, Data Processing Center. Direct mailings of a computer-generated letter are sent to recently-discharged veterans, accompanied by a pamphlet describing available benefits. Six months later a follow-up letter is sent.

Emphasis is placed on outreach to aging veterans, former prisoners of war,

female veterans, and disadvantaged veterans. Disadvantaged veterans are identified at the time of the VADS mailing and sent appropriate materials. In 1981 the VA law was changed to relax eligibility requirements for former POW's, and to extend the benefits period. A hotline has been installed for use of former POW's to enable them to notify the Central Office if treatment by the VA has not been consistent with the new legislation. Due to the special outreach efforts, nearly all former POW's have been contacted and advised of their rights.

Since the veteran population as a whole is aging, VA benefit programs are becoming more involved with older veterans. The VA is participating in a working agreement with other Federal agencies to provide information and referral services for senior citizens. Outreach to female veterans has taken place primarily at the regional level. Veterans' organizations with large female memberships have been identified and contacted.

Technology Impact. There are long-range plans for the automation of this office. None of the plans are concrete enough to be commented upon at this time.

DATA ANALYSIS AND SYNTHESIS

The Veterans Administration must deliver benefits and services to a constituent base that numbers in the millions. The programs of benefits and services are many and varied. To consistently deliver a variety of benefits to a large number of persons, the VA has relied on computerized systems for some time. Like other agencies, however, the automation of office functions has just recently arrived at the Veterans Administration.

The criteria developed for this study to assess civil liberties impact were applied to information handling practices at the VA. As before, the three areas of civil liberties impact were: public access to rulemaking, personal and company information practices, and the dissemination of public information.

1. Constituencies Affected. The first criterion concerns the constituencies that are affected by agency policies and practices, especially those involving the use of information technology. The VA's constituency is, of course, veterans; also included are survivors and dependents. In 1983, the VA identified the following special constituencies: the aging veteran, persons affected by Agent Orange, and female veterans. Veterans, veteran groups, and academic and government users all benefit from VA statistical services.

A service program of the magnitude of the VA's could not exist without the

information technologies used. The trend toward automation of internal systems should also result in more efficient delivery of services and benefits.

2. Public Meetings and Comment on Proposed Rulemaking. Information technology has not affected the provision of public access to the rulemaking process. There is no information about any changes in numbers or types of meetings. Notices of meetings and proposed rulemakings are still published in the Federal Register. Comments are still received by conventional means. The targeting of special groups like Agent Orange victims usually involves the establishment of advisory committees. The existence of advisory committees and the provision of access to their meetings and reports generally serves to increase public input to the decisionmaking process.

The development of ARMIRS, the electronic version of VA regulations, could be used as a tool to increase public access to the rulemaking process. However, there are no plans to allow public use of the data base.

3. Dissemination of Publications. Veterans Administration printing plants are being closed out. There is no data available on the effect, if any, the closings will have on the number or type of publications issued. The Department of Medicine and Surgery was ordered to make a 25 percent cutback in pamphlets describing VA research and programs in various medical areas. No budget cuts were applied to statistical documents issued by the Office of Information Management and Statistics.

Research studies have not been sufficiently controlled to assess any change in number or type.

New technologies have not been applied to publication dissemination for the most part. Electronic publishing is not contemplated at this time. Few of the veteran constituents would have a need for computerized data bases, but academic and government consumers of VA statistics might. The Department of Veterans Benefits does have a Veterans Assistance Program which utilizes computer mailing to distribute pamphlets to recently discharged veterans.

4. Contracts for Dissemination. Some VA research studies are published by National Technical Information Service. Since the closing of the Central VA printing plant in October 1984, most of the VA's printing has been performed by contractors selected by GPO. Most technical functions of the VACO library are contracted out. There are no other contracts for information dissemination.

5. Library Closings. Not applicable.

6. Marketing. Outreach programs, particularly to special emphasis groups like Agent Orange and Former Prisoners of War, market VA benefits and services to prospective beneficiaries. The increased focus on special groups, and changes in

the laws have resulted in enhanced marketing by Public Affairs and DVB staff, but no quantitative documentation is available. However, the DM&S publications that were cut back were regarded by agency management as public relations materials.

7. Personal and Company Information Rights. The VA collects a large amount of personal information for its medical and benefits data bases. Much of the information is only accessed for statistical purposes. Other uses of the data include computer matching, modeling and profiling, release of names and addresses, personal computer access, and debt reporting. Although all of these activities contain the potential for abuse, the Veterans Administration does not appear to be infringing on personal information rights.

Release of names and addresses only takes place under controlled circumstances authorized by statute. The computer model employed by the Office of Information Management and Statistics is solely used for statistical projections of the veteran population. Downloading of data into personal computers does not take place on a large scale at present. The reporting of delinquent debts is not in place yet—it will be implemented in 1986.

Computer matching has become an effective tool for audits conducted by the Office of the Inspector General. They appear to be conducting matching studies in a responsible manner in accordance with OMB guidelines. Raw hits are refined by computer, then verified by program personnel. Persons turned up as possible recipients of overpayments are given an opportunity to dispute the claim and update the records.

Use of matching data to develop a profile of potential abusers of the pension system could have civil liberties ramifications, if the profile was then used to limit benefit rights. As of the date of this report, no profile had been isolated.

8. Security Procedures. Adequate procedures and policies are in place to ensure the security and integrity of data kept on mainframe systems. Committee meetings are being held to address the issue of microcomputer security. Although written procedures are considered applicable to small systems, they do not necessarily address all the issues peculiar to microcomputer uses. Computer training given at the Information Technology Center emphasizes microcomputer security problems, but cautionary advice is not equivalent to control.

TOPICS FOR FURTHER RESEARCH

- Security and integrity of data maintained on or accessed by

microcomputers. This issue grows in magnitude as the agency strategy of increased user access is implemented.

o Electronic mail issues: once the automation of office functions is more fully underway, as outlined in the attachment "Automation of Administrative Processes," use of the integrated network should be more fully investigated. The same issues of integrity and security apply, as well as problems of authentication. The Office of Public and Consumer Affairs contemplates the use of electronic mail to vary the attribution of statements on press releases to the field.

o Computer matching projects have generated a number of issues: If forecasting ever becomes operational, it should be investigated. Special concern should be given to matches that employ data of an especially private nature, such as the data on persons deemed unemployable for mental health reasons. Proposed legislation to authorize the use of IRS files should be researched.

o Delinquent debt reporting under the Debt Collection Act is a controversial issue and bears further investigation once the VA project is operational.

5. A COMPARISON OF AGENCY PRACTICES

This section presents a comparison of agency information/technology practices in the three civil liberty areas considered for this study. A summary of findings is depicted in Table 2. Before comparing the agency practice, an overview of the technology environment of most agencies is described.

5.1 THE TECHNOLOGY ENVIRONMENT

In general, agency computer environments can be described as a mixture of mainframes, with minicomputers and microcomputers. The age of the equipment also varies, so that many agencies are running both old and new equipment. Most computer centers house mainframes and provide time-shared access, as well as batch processing. They are responsible for data security only on the mainframe, but once the data is downloaded to a micro, security becomes a local issue. Many activities at the program level are run on minicomputers, and all agencies are experiencing an increasing influx of micros. In Energy, for example, an acquisition of 4,000 microcomputers is expected in the Washington Computer Services Center. USDA projects 10-15,000 micros in use by 1985. Agencies are also using a variety of networking and messaging systems for voice and data communications.

The single most important factor in the technology environment is the microcomputer because it puts the power of information collection, storage, manipulation, processing, retrieval, transfer and printing into the hands of the individual and raises security, productivity, and management issues about information resources that have either been dormant or irrelevant in other media forms.

IRS is an exceptional case because they can afford to and are experimenting with a variety of information technologies: portable lap computers, artificial intelligence, and optical disk technology. However, their daily work environment is similar to the rest of the Federal agencies, as they operate with typical mainframe, mini and office automation equipment.

5.2 DATA PROTECTION/PRIVACY/CONFIDENTIALITY

Information is collected on individuals and/or companies in all of the agencies which were part of this study. With respect to the way information technologies impact agencies' handling of information on individuals and companies, it is useful to look at the following topic areas: computer matching, FOIA, security, electronic records management, debt reporting and information and data sharing/transfer.

Matching. In four of the seven agencies (USDA, IRS, LABOR, VA) matching has become a routine practice used to initiate, administer, and/or audit programs. IRS

TABLE 2. SUMMARY OF FINDINGS ABOUT INFORMATION/TECHNOLOGY PRACTICES IN THREE CIVIL LIBERTIES AREAS

DATA PROTECTION/PRIVACY/SECURITY

Matching
— Has become routine practice used to initiate, administer, audit programs in: USDA, IRS, LABOR, VA.
— Is done mostly at state or regional levels, not under direct observation of national/Federal office.

FOIA
— FOIA process not affected by technology—the focus is on information content.
— Computerized records facilitate responses.
— Responses are completed manually in all agencies.

Security
— Biggest issue is data protection on micros.
— Manuals in agencies primarily address mainframes, minis—not micros.
— Individual training on security is formal and informal--mostly seen as local management responsibility.
— Security procedures functionally overlap with electronic records management procedures.

Electronic Records Management
— Electronic records management procedures are missing from and needed by all agencies— especially in disposition and definition of record copy.
— Signature chain on electronic records is an issue. USDA is conducting experiment here.

Debt Reporting
— Primarily an issue for agencies issuing loans (VA, SBA, parts of USDA not studied).
— SBA programs are operational, VA to follow.
— Involves downloading and financial privacy questions.

Data Sharing/Transfer
— Use of mail still widespread for document and tape transfer. Biggest issue is micro- mainframe connection for up/downloading. Found in USDA, ENERGY, IRS, LABOR, SBA, VA.
— Minicomputer networks in place over a decade; still heavily used.
— Conflicting policies on disclosure vs confidentiality found in Energy and IRS.
— No documented procedures found regarding electronic transfer in: Federal/State partnerships for program administration; national/regional/field office delegation of Federal responsibilities.

DISSEMINATION OF PUBLIC INFORMATION

Printing Cuts
— Printing cuts (esp. in response to OMB Bull 81-16) found in: USDA, CPSC, SBA, VA.

— Constituencies affected: farmers, agriculture sciences researchers, general public with interests in food & nutrition, schools; consumers, small businesses, veterans, the press.

Dissemination Fees
— Varies by agency, program, and media. Some documents are free (in IRS, CPSC, parts of LABOR); others for a fee (USDA, SBA).

— All electronic dissemination has a charge.

Info Center/Library Cuts
— Varies by agency. Cuts in LABOR, CPSC. Contracting out widely practiced. No increases found.

Electronic Dissemination
— Electronic dissemination is in effect or in planning in: USDA, ENERGY, IRS, LABOR, VA.

— Accelerated by cuts in printing.

— New, "technology literate" public is required.

A-76 Issues
— Contracting to private sector widespread across agencies.

— Issues traditionally not a matter of technology but of policy and budget.

— USDA experience raises questions of unfair competition from contracting out electronic publishing.

ACCESS TO RULEMAKING

— Technology has not altered number or type of public meetings.

— Notice of hearing still done via Federal Register and public comments continue to be submitted through conventional means.

conducts matching of its own records, as well as with private sector firms (for real estate sales and household mailing lists) and other government agencies. In USDA and LABOR it is conducted primarily at the State and local levels; in the VA, at regional or local offices as well as the Central Office. The Federal agency is not responsible for specific procedures used in these many locations, except to oversee that they comply with the Privacy Act and Federal regulations governing confidentiality and disclosure. SBA was once involved in a matching activity in the 1970s, but has since stopped the practice. The Department of Energy does not conduct matching, but it will provide data to other agencies to fill a significant request.

In short, matching has become part of managing government programs and it appears to be a permanent procedure. The extent to which matching has become routine needs to be documented. In addition, it appears that the lines of responsibility for matching procedures used by state and local authorities for Federal programs do not appear to be clearly defined or documented. Does Federal law override state in all cases? Who is responsible for privacy and data protection at the local levels? Before raising this as an issue, more attention is needed to determine the extent to which responsibility for matching has been spelled out for regional, State, local, and field offices carrying out Federal programs.

FOIA. The FOIA process is not affected by technology. Agencies follow closely the letter of the law and the focus is on information content. That "content" can be requested whether it resides on paper, microform, computer tape or floppy disk. It was found that FOIA personnel support computerized records because it facilitates their retrieval of documents requested. FOIA responses are still completed manually in all agencies; i.e. information is not sent electronically in answer to a request.

Security. Computer security has been a concern to the Federal government for decades. All agencies produce security manuals, mostly addressing mainframe and minicomputers with respect to software and hardware controls, audits, and physical security. Microcomputer security is seen as a separate issue, and in all agencies it is unresolved. It is being addressed in USDA, Energy, IRS and VA. DOE has conducted studies of software which provides security for microcomputers, but no software has been found completely adequate for DOE needs. An additional concern for the microcomputer use at DOE is the ability to provide physical security to remote, stand-alone systems. At the Department of Labor, there is great concern about protecting the integrity of the data in large data bases against

unauthorized access and use at the microcomputer level. Data can be downloaded onto a microcomputer system, processed, and returned to the data base without immediate detection of changes to the data base files. Securing microcomputer systems against unauthorized access and use is also a great concern at the Department of Energy. IRS' Automated Examination System will employ portable computers which will access the master computer files. If these portables also have the capacity to store data, the security problems will be amplified.

There is no standard, formal training program for government employees on computer security practices. Training programs vary as follows: some agencies conduct formal programs, as in Energy where security and privacy training is conducted as a mandatory orientation program; others use informal approaches, such as in IRS where computer security is made part of other functions and given to managers as a supervisory responsibility; still others mix formal and informal, as is the case in LABOR where OASAM provides training on security and privacy as part of a general orientation program while the Office of Program and Fiscal Integrity conducts regular seminars on privacy and confidentiality issues.

The most significant indicators in this area are: whether agencies are aware of microcomputer security as an issue; what actions are being taken to understand and address these issues; whether guidance is needed in the form of standards from NBS or guidelines from GSA.

Data sharing/Transfer. The use of the mail is still widespread in sending documents and computer tapes. Minicomputer networks have been in place for over a decade, and continue to be heavily used. The biggest issue in this area is mainframe-microcomputer downloading/uploading. Once the data is downloaded to a micro from the mainframe, responsibility for security, access, dissemination, maintenance, integrity becomes local. For many Federal functions, especially administrative functions covering millions of employees, downloading could be a great technique for productivity. For example, payroll- personnel data is collected, manipulated and owned in the divisions, branches and programs of each agency, but checks get written from a central source. As planned by USDA, micro-mainframe connections would be most effective in computing and transferring this data. However, security and confidentiality become primary concerns. Security surrounding micro-mainframe connections has become an issue in every agency except CPSC, which is not yet computerized.

Another information transfer area requiring attention is electronic mail. The technology for electronic mail allows voice and data to be easily transferred, and

brings up a potential conflict between efficiency and productivity on the one hand, and security concerns on the other. Electronic mail systems generally provide password protection, but are not considered "secure." They are used primarily for informal messaging, but could be used to transfer information of any sort, provided it is online. Further documentation is needed to document the extent of electronic mail use; what types of information are being transferred on the system; and what practices are being used to deal with security and access.

It is important to document further the extent to which agencies are planning and practicing micro-mainframe connections; whether they see downloading as a security problem; what practices they are evolving to resolve this issue.

In addition, no specific procedures were found which define electronic information exchanges between agency HQ and their regions/field offices, and between national and state governments. This indicator also needs additional follow-up work.

Sometimes agencies develop or are under conflicting policies for data sharing. For example, within ENERGY, the EIA is under legislative mandate to share its data with other components of Energy, specifically the Federal Energy Regulatory Commission, and with other government agencies including the Department of Commerce. The concern is that the requesting agencies may not be able to protect the confidentiality of the requested data. Similarly, IRS under Title 44 is required to submit its permanent records to NARS, but under Title 26 is required to protect confidential taxpayer information. It would be informative to document the extent to which conflicting requirements are placed on agencies in this area of data sharing.

Debt Reporting. The Debt Collection Act of 1982 states that agencies may disclose confidential consumer loan information to consumer credit reporting agencies. OMB Bulletin 83-21, issued September 21, 1983, requires all agencies to report commercial debts and delinquent consumer debts to private sector credit agencies, and to establish procedures for using credit reports as a part of the decisionmaking process when awarding loans, contracts and grants. The Veterans Administration has concrete plans to implement debt reporting. SBA has current contracts with Dun & Bradstreet for debt reporting by magnetic tape. Dun & Bradstreet will be able to download this information to smaller, local credit bureaus where units may not be equipped to deal with considerations of security, access, dissemination and integrity. Because of the use of information from systems of records deemed confidential under the Privacy Act, and the data downloading issue,

Federal debt reporting is a controversial area in the financial community and it is an area that requires attention from civil liberties perspectives.

Electronic Records Management. Records management procedures for machine-readable records, especially in records disposition practices and in the definition of "record copy", are missing and needed in all agencies. No agency appears to know how to manage electronic records. In USDA and ENERGY, the signature chain on official records was raised as an issue. Records management also deals with intellectual and physical access procedures and overlaps the issues raised under security.

5.3 DISSEMINATION OF PUBLIC INFORMATION

Public information is disseminated through a variety of media, including hard-copy publications, microfiche, audio-visual materials, and computer and communications technologies. Comparative statements about the impact of information technologies on the dissemination of public information must take into account policy and budgetary issues as well as technological concerns. Comparisons have been drawn on the following topics: cuts in budgets for printing expenditures, fees for dissemination of public information, information center/library cuts, electronic dissemination, and the A-76 Issues.

Printing Cuts. Four of the seven agencies reported significant printing cuts in their budget and operations: USDA, CPSC, SBA, VA. The Director of Publications at USDA described the cuts as a response to OMB's 1981 moratorium on printing. As a result 1400 publications were eliminated, several hundred others combined, and a new policy eliminating free publications was instituted. In the short run, he believes the cut is affecting traditional USDA constituencies. It is hard to project over a longer time period or to know whether other organizations will fill the publications void. The printing cuts should not be viewed as a causal force in initiating electronic publications, as USDA is generally searching for appropriate and productive computer applications. But it has served to accelerate electronic publishing applications.

The Veterans Administration printing plant has been closed down. Patientprinting shops operated as a part of vocational rehabilitation are being phased out. Informative pamphlets produced by the Department of Medicine and Surgery were cut back 25%. No electronic publishing is planned.

At CPSC, all outreach activities were cut back. Publications and other services of the Outreach Coordination Office were curtailed because of reductions in force and budget restrictions.

Parts of the Small Business Administration were hit by printing cuts also. The Management Assistance Office of SBA was forced to reduce the number of titles published from over 800 to 200.

In the publications area, printing cuts and numbers and types of constituencies affected by cuts can be viewed as indicators of potentially negative effects on information dissemination. These indicators need further documentation and analysis.

Dissemination Fees. The policy for charging fees for disseminating information to the public varied by government agency, program, and media. In a few government agencies or program areas, information is disseminated free, such as reported by IRS. Also the National Occupational Information Coordination Committee makes funds available to establish programs (through State agencies) to disseminate occupational and career information free to the public.

Other agencies and programs charge fees for the information disseminated to the public. Pricing policies vary by agency and program areas. The Energy Information Administration (EIA) sells its publications through the Government Printing Office and the National Energy Information Center on a cost recovery basis. A relatively recent policy at USDA is to charge for all information except in rare cases where dissemination is integral to the program. This is a significant change for USDA constituencies, which have previously had access to free publications. Both VA and CPSC continue to offer their publications at no charge. The Small Business Administration continues their previous policy of selling some documents to the general public and distributing others for free. With the 1981 change in management at GPO came a considerable increase in the prices charged for SBA publications. All publications are free to clients receiving management assistance counseling at SBA.

All electronic dissemination of information has a charge. Access is usually through a commercial data base vendor, and fees are set in accordance with the vendor's system usage charges.

The practice of charging for government information dissemination reflects difficult choices regarding budgetary considerations and cost recovery requirements on the one hand, and the public's need/right to know, on the other hand. This area can also be viewed an an indicator of issues that Congress needs to monitor.

Library/Information Center Cuts. The concerns here varied by agencies. No agency reported an increase in library/information/center activity. Many agencies are contracting out this function. At the Employment and Training Administration, contracts for libraries/information centers had been eliminated over the past

two-three years. CPSC library staff was cut back severely during the same period. All library functions are currently being contracted out, except for the reference and administrative duties performed by the one remaining staff person.

Electronic Dissemination of Information. In the majority of agencies, electronic dissemination is in effect or in the planning stages. At the Department of Energy, the Technical Information Center maintains the DOE/RECON data base for online access to information about technical and scientific reports. The National Occupational Information Coordinating Committee (ETA) is now funding grant agreements to make occupational information systems available not only through remote access to mainframe computers but also through portable and stand-alone microcomputer systems. The Office of Information and Public Affairs is planning to use the DIAL-COMM system as a means of electronically disseminating press releases to the news media.

At USDA, electronic dissemination has just been initiated in a project to publish four major reports on agricultural marketing, economic forecasts, crop statistics and foreign trade leads. The project initially met with controversy from small agricultural data publishing firms concerned about unfair competition. USDA officials met with the Information Industry Association and Glenn English's staff. Difficulties were resolved, for the project is now in progress and Martin Marietta has the USDA contract. This experience reflects that contracting out electronic dissemination could result in impacts different from document publication. It is worthy of further investigation.

The Office of Public and Consumer Affairs at the VA also intends to implement electronic dissemination of press releases. Although VA and the other independent agencies profiled (CPSC and SBA) all maintain computerized statistical data bases inhouse, there are no plans make these available to anyone else.

IRS is experimenting with electronic dissemination of its most sought after publications by making them available to data base vendors and telecommunications services who want to pay the fee for the tapes and who are willing to collect usage statistics for IRS.

A-76 Issues. Traditionally, the issues involved in contracting to the private sector have been a matter of policy and budget, not of technology. Contracting to the private sector is widespread across all agencies and programs. Most of the large information systems in both the Department of Labor and the Department of Energy are maintained and secured by private sector contractors. For the most part, the smaller agencies profiled maintain their own information systems. SBA does employ

a number of contractors both outside and within SBA for projects of the Office of Computer Science. There is also significant cross-agency contracting in the dissemination area, with many types of publications activities contracted to GPO. The extent to which GPO contracts conflict with A-76 policies was not raised by interviewees, but is an issue to consider.

Most libraries contract library technical services. Both CPSC and SBA have contracts for distributing publications. Management Assistance within SBA has many of its publications written by contractors. The IRS policy has been not to contract out technical writing of publications because the text of many of its documents hinges on internal decisions and strict clearance procedures.

As discussed above, contracting for electronic dissemination appears to have potentially new impacts on competitiveness in the marketplace and should be studied further.

5.4 ACCESS TO RULEMAKING

Technology has not altered the number or type of public meetings held. Notice of hearings still are published in the Federal Register and public comments continue to be submitted through conventional means.

6. PRESENTATION AND DISCUSSION OF TOPICS FOR FURTHER RESEARCH

In considering topics for further research, it is important to recall that the overall objectives and context of this study deal with providing policy guidance to Congress with respect to information and technology practices in the three civil liberty areas of data protection, public information dissemination and access to rulemaking. In this project, too few agencies and/or programs were studied to define policy options for Congress, but the comparison of agency practices has served well to conceptualize potential issues and raise questions that, if further documented, would provide a basis for suggesting new or revised policies. These issue areas are presented below along with suggested specific questions that should be addressed in future empirical studies. It should be noted that no issues arose under "access to rulemaking," as this function appears to be still unaffected by technology.

DATA PROTECTION/PRIVACY/SECURITY

Matching. Matching has become or is becoming a necessary procedure in administering many Federal programs and accomplishing many Federal missions. Because it involves individual/company identifiers, it will always carry a potential threat of privacy infringement. Policies and guidelines for matching responsibilities and procedures are inconsistently documented. Federal and state agency officials are primarily following the Privacy Act, precedence set in past disclosure cases, and their own needs for security and confidentiality. In some agencies, notably LABOR and USDA, most of the matching is done by state agencies administering Federal programs. In these cases, the Federal officials have little direct observation or specific documentation on the policies, procedures and responsibilities employed in the states which conduct matching. In other agencies, such as IRS and VA, where matching is both conducted at HQ, and also decentralized, but to regional or local field offices, a similar situation exists. In all cases, Federal authorities conduct program audits, in which matching is reviewed along with other procedures, and it is generally under such audits that difficulties/problems would be detected.

Before suggesting any policy options in this area, it is necessary to:

- Document extent of matching used by agencies.

o Document matching practices in the agencies, including:

- purposes for which matching is used
- where conducted and by whom
- documentation of responsibilities, policies, procedures

o Review documentation (guidelines and policies)

o Analyze Federal-state relationships/interactions with respect to matching

o Analyze HQ-regional/field offices relationships/interactions with respect to matching

o Determine to what extent matching is part of program audits, and whether it is a specific audit area.

Microcomputer Security. Security procedures surrounding use of the microcomputer are not well defined in the agencies/programs and represent a significant challenge to Federal administrators. Microcomputers offer the potential means of productivity and efficiency to every individual employed by the Federal Government. Their use by these millions of people raise many questions about data protection concerning access to records previously controlled manually. This is especially significant in mainframe-micro downloading of records and files, where previously secured data becomes available to many individuals no longer under the control of the data center. Data integrity is very much a part of the security problem, for once downloading occurs, and there is no date attached to the currency of the records, there are many opportunities to transfer inaccurate data. No agency has resolved the security issues surrounding use of the micro.

In addition, there appears to be no consistent, formal training on security for individuals using microcomputers. Training responsibility is also considered a local function of Federal managers.

A specialized area under microcomputer security involves use of the portable, lap computer, a technology which not only allows access via modem of central data bases, but allows that data to be carried out of the official Government office and into many uncontrolled, insecure areas. Special security considerations and management attention are needed for appropriate use of this technology.

Before considering policy options, it is necessary to:

o Determine what the lead agencies under the Brooks Act (NBS, OMB, GSA, GAO) are doing with respect to providing guidelines and/or standards for microcomputer security.

o Document the extent to which microcomputer security is an issue in the agencies, including:

Types of data allowed on the micro
Access policies and procedures
Security conditions favoring floppies vs hard disks
Software, hardware and physical security measures used
Training programs in place or planned for micro security

o Document the extent to which lap computers are being used, including:

[Same topics listed above]

Electronic Information Transfer. Electronic information transfer covers many issues dealing with specific technologies, institutions, and laws/policies involved in transfer. The two technological processes which have significant bearing on these issues are micro-mainframe connections and electronic mail. These technologies raise many of the issues discussed above under the security section. Electronic transfer encompasses many types of institutions/organizations and raises questions about responsibility and authority surrounding interactions between: agency HQ and regional/field offices, as well as HQ and components or subagencies; interagencies; Federal authorities and state governments. Because the scope and types of transfers increase so greatly from using the micro-mainframe and electronic mail technologies, it is important that parties involved in the transfer know responsibilities and not take the transfer process for granted.

One other issue under this topic is the nature of legislative or policy inconsistencies that relate to data sharing and privacy. Two inconsistencies were found among the seven agencies/programs profiled: one in Energy, dealing with EIA's mandate to protect and share data and FERC's to disclose; and the other in IRS, dealing with its requirement to protect information as it conflicts with NARS requirement to archive and make public agency records. A thorough understanding and documentation of such inconsistencies would help Congress avoid or reduce them in the future.

In order to develop policy options in this area, it is necessary to:

o Document the extent to which micro-mainframe connections are in place or being planned.

— Focus on payroll/personnel and budget programs because they are such likely candidates for micro-mainframe up/downloading
— Include security questions listed above.

o Document the extent to which electronic mail is used, including

- For what purposes
- Between and among what offices/levels in the bureaucracy
- Security measures planned or in place
- Security responsibilities assigned to the parties in the exchange
- Types of information transferred

o Document the extent of inconsistent laws, regulations, policies, and practices regarding data/information transfer, protection and disclosure.

Debt Reporting. Debt reporting is an issue in agencies involved in loans. It inherently involves the transfer and manipulation of records deemed confidential under the Privacy Act, and therefore carries potential security risks. Debt reporting is increasingly easier to enact through computer networking of various types. Responsibilities and procedures for security, access, and data integrity need to be clear to parties involved in the transactions.

In order to formulate policies in this area, it is necessary to:

o Document where debt reporting is practiced and what parties are involved

o Document the extent and type of electronic transfer used,including:

- Types of information transferred
- Security issues (Same as listed under security section)
- Security responsibilities assigned to parties involved
- Documentation of procedures.

Electronic Records Management. All agencies/programs profiled in this study reported the lack of and need for procedures to manage machine readable records. Records management is intricately intertwined with issues of records security, as control and access are basically governed by records management practices. Three of the most significant issues include disposition of electronic records, the definition of electronic record copy, and handling the signature chain on electronic records storage and transfer. In order to specify policies in this area, it is necessary to:

o Review and analyze what is being done or planned in NARS and in OIRM/GSA to offer guidelines and/or standards to the agencies.

o Document the extent to which electronic records management is an issue in the agencies.

o Document what agencies are doing to handle electronic records management:

- storing, maintaining, disposing of digitized records
- applying disposition schedules to electronically stored files

— applying cost/benefit conditions to choices of record storage and output
— applying the signature chain to electronic records
— controlling intellectual and physical access for different users (managers, staff, NARS, historians, FOIA officers).

Other Technology Issues. A few agencies are experimenting with a host of technologies, including artificial intelligence, optical disk technology and various combinations of applications and computer capabilities (e.g. IRS). These experiments reflect the beginning of issues to come and should be documented so they can be monitored and researched on a continuing basis.

DISSEMINATION OF PUBLIC INFORMATION

Printing Cuts/Constituencies Affected. Cuts in printing affect civil liberties areas when they hinder constituencies' ability to obtain public information. In some agencies, printing cuts have eliminated hundreds of documents. The specific impact on constituencies is difficult to quantify. In order to view this issue as an indicator of potential infringement, it is necessary to:

o Document the extent of printing cuts in agencies and

o Relate printing cuts to constituencies affected.

o Document the extent to which printing cuts affect the incidence of electronic publishing.

Library and Information Center Cuts/Constituencies Affected. Cuts in library/information center operations and programs affect civil liberties areas when they hinder constituencies' ability to obtain public information. The nature of the impact of such cuts is also difficult to quantify. In order to view this issue as an indicator of potential infringement, it is necessary to:

o Document the extent of information center cuts in agencies/programs and

o Relate cuts to constituencies affected.

Dissemination Fees/Constituencies Affected. Whether charging for government dissemination of information is an issue under civil liberties also depends on the nature and extent to which constituencies are negatively affected. Fees are not new to the Federal Government's publication programs. There is a charge on most of GPO and NTIS documents. In many cases, charging policies in agencies amount to dissemination through either GPO or NTIS. Whether any changes have occurred over the past four years regarding access to GPO or NTIS publications was not reviewed during this project. In order to view this issue as an indicator of potential

infringement, it is necessary to:

o Document the extent to which agencies are charging forpublications and

o Relate to constituencies affected.

o Review policies and practices of GPO and NTIS, perhaps in case studyapproaches dealing with agency/NTIS or GPO relationships.

Electronic Dissemination/Constituencies Affected. Electronic dissemination requires computer equipment at the user's end and implicitly requires a certain level of training/education to use such an application, as well as the financial means to provide the equipment. The "electronic-oriented constitutency" may or may not differ from the traditional consdituency in the dissemination of certain information and documents. In order to view this area for policy implications, it is necessary to:

o Document the extent to which agencies are using electronic dissemination and publication and

o Determine whether alternative choices of dissemination are being offered to constituencies and

o Assess whether constituencies are negatively or positively affected.

A-76 Issues. A-76 is an OMB policy that requires the Federal Government to contract with the private sector for services performed more efficiently by that sector. Agencies profiled in this project are all contracting out information services of various sorts. The only potential issue arose in USDA, where an electronic dissemination contract was questioned as giving a monopoly to the firm awarded the contract. In order to determine if this is an issue that warrants attention, it is necessary to:

o Identify electronic dissemination/publication projects in the Federal Government and

o Determine if questions of monopoly or small business infringements arose.

7. BIBLIOGRAPHY

Acts, Regulations and Policies

Administrative Procedures Act (5 U.S.C. Sections 551 and 553-559, 1966; amended 1976).

Analysis of Regulatory Functions Act (5 U.S.C. Sections 601-612, 1980).

Brooks Act, 1965. PL 89-306.

Debt Collection Act of 1982, P.L. 97-365.

Distribution and Sale of Public Documents (44 U.S.C. Section 1701-1722, 1968; amended 1977, 1982).

Fair Credit Reporting Act (15 U.S.C. 1681 et seq.).

Fair Debt Collection Practices Act (15 U.S.C. 1692 et seq.).

Federal Advisory Committee Act (5 U.S.C. App. Sections 1-15, 1972; amended 1976, 1980 and 1982).

Federal Claims Collection Act (31 U.S.C. 952; 1966).

Federal Information Resources Management Regulations, 41, CFR 201.

Federal Manager's Financial Integrity Act of 1982.

Federal Program Information Act. PL 95-220. December 1977. (31 U.S.C. 1701).

Federal Property Management Regulations, 41 CFR 101. FIRMR Subparts 201-35.3 and 35.17.

Freedom of Information Act (5 U.S.C. Section 552, 1966; amended 1967, 1974, 1976 and 1978).

Inspector General Act of 1978, from Appendix to Title 5, 1981 Supplement. PL 95-452.

OMB Circular No. A-71. Responsibilities for the Administration and Management of Automatic Data Processing Activities. Washington, DC: 1965.

OMB. Circular No. A-76. Transmittal Memorandum No. 7 from David A. Stockman. Policies for Acquiring Commercial or Industrial Type Products and Services Needed by the Government. Washington, DC: 1982.

OMB Circular No. A-108. Responsibilities for the Maintenance of Records About Individuals by Federal Agencies. Washington, DC: 1975.

OMB Circular No. A-123. Internal Conterol Systems. Washington, DC: 1981. (Revised 1983).

OMB Bulletin 81-16. Elimination of Wasteful Spending on Government Periodicals, Pamphlets and Audiovisual Products. 1981. Supplement. Elimination and Consolidation of Government Periodicals and Recurring Pamphlets. Washington, DC.

OMB Bulletin 83-21. Implementation of Debt Collection Act of 1982—Use of Credit Reporting Agencies. Washington, DC.

OMB Privacy Act of 1974—Revised Supplemental Guidance for Conducting Matching Programs, Federal Register, Vol. 47, No. 97.
Paperwork Reduction Act (44 U.S.C. Sections 3501-3520, 1980).

Privacy Act (5 U.S.C. Section 552a, 1974; amended 1975, 1982 and 1983).

Records Management by Federal Agencies (44 U.S.C. Sections 3101, 3107, 1968; amended 1976).

Records Management by Administrator of General Services (44 U.S.C. Sections 2901-2909, 1968; amended 1976).

Social Security Amendments. PL 95-216. December 20, 1977. (42 U.S.C.. 1305).

Sunshine Act (5 U.S.C. Section 552B, 1976).

Tax Reform Act, 1976 (26 U.S.C). PL 94-455.

Trade Secrets Act (18 U.S.C. Section 1905, 1948; amended 1980).

Books, Monographs, Reports, Journal and Newspaper Articles

Abelson, P.H. and Hammond, A.L. The electronics revolution. Science (195) 8, March 18, 1977.

Barringer, Felicity. OMB Bid Advances to Screen Agency Rules.The Washington Post, December 21, 1984, p. A4.

Becker, Louise Giovane. Federal Information Management Policy: Critical Directions. Congressional Research Service, Library of Congress. Washington, DC: 1981.

Becker, Louise Giovane. Computer Security: An Overview of National Concerns and Challenges. Congressional Research Service, The Library of Congress. 83-135-SPR. Washington, DC: 1983.

Belair, Robert R. 1981. Access to Information. Chapter II of Issues in Information Policy, National Telecommunications and Information Administration Special Publications.

Bell, Daniel. 1973. The Coming of Post-Industrial Society. NY: Bantam Books.

Bortnick, Jane. Computer Crime and Security. Congressional Research Service, The Library of Congress. IB80047. Washington, DC: 1984.

Bulletin of the American Society for Information Science. Congress in the Information Age. Vol. 1, No. 9. April 1975.

Carlson, Walter M. Privacy. 1977. Privacy. In Martha E. Williams, ed. Annual Review of Information Science and Technology. Vol. 12. American Society for Information Science. White Plains, N.Y.: Knowledge Industry Publications, Inc. pp.279-305.

Chartrand, Robert L. Congressional Management and Use of Information Technology. Journal of Systems Management, August 1978.

Chartrand, Robert L. and Jean Paul Emard. Information Systems and Automatic Data Processing (6th Edition) Selected References. Congressional Research Service, Library of Congress. TK 6565 C. Selected References. Washington, DC: 1975.

Chartrand, Robert L. The Legislator as User of Information Technology. Congressional Research Service, Library of Congress. 77-217 SP. JF 522. Washington, DC: 1977.

Culnan, Mary J. "The Impact of Technology on Public Access to Information," OTA Background Paper, July 1984, unpublished.

DeWeaver, M.J. 1984. The role of libraries in creating and providing viewtext information services. Bethesda, MD: ERIC, Vol. 1, ED 243497; Vol 2, ED 243498.

Ehlke, Richard. Federal Protection of Trade Secrets and Proprietary, Commercial and Financial Information Obtained by Government Agencies in the Context of Energy-Related Data. Congressional Research Service, Library of Congress. 77-226A. 654/126. Washington, DC: 1977.

Ehlke, Richard C., and Harold C. Relyea. Freedom of Information Act Amendments. Congressional Research Service, The Library of Congress, IB82003. Washington, DC: 1984.

General Accounting Office (hereinafter cited as GAO). A Bibliography of Documents Issued by the GAO on Matters Related to: ADP. Washington, DC: 1981.

GAO. A Bibliography of Documents Issued by the GAO on Matters Related to: ADP. Washington, D.C.: 1982.

GAO. A Bibliography of Documents Issued by the GAO on Matters Related to: ADP. Washington, DC: 1983.

GAO. Informing the Public About Food--A Strategy is Needed for Improving Communication. Washington, D.C.: 1982.

GAO. Better Information Management Policies Needed: A Study of Scientific and Technical Bibliographic Services. Report to the Congress of the United States by the Comptroller General. PSAD 79 62. Washington, D.C.: 1979.

GAO. Observations on Collection and Dissemination of Scientific, Technical, and Engineering Information. Report of the Comptroller General of the United States. GGD-76-75. Washington, D.C.: 1976.

GAO. Education Paperwork Requirements Are Burdensome: Better Federal Controls Needed. GGD-82-28. Washington, DC: 1982.

GAO. Small Businesses Are More Active as Inventors Than as Innovators in The Innovation Process. PAD-82-19. Washington, DC: 1982.

GAO Misuse of SBA's 8(a) Program Increased Cost for Many ADP Equipment Acquisitions. AFMD-82-9. Washington, DC: 1982.

GAO. Informing the Public About Food--A Strategy Is Needed For Improving Communication. CED-82-12. Washington, DC: 1982.

GAO. Department of Agriculture Needs Leadership in Managing its Information Resources. CED-81-116. Washington, DC: 1981.

GAO. Electronic Marketing of Agricultural Commodities: An Evolutionary Trend. RCED-84-97. Washington, DC: 1984.

GAO. Public and Private Efforts To Feed America's Poor. RCED-83-164. Washington, DC: 1983.

GAO. Federal Food, Agriculture, And Nutrition Programs in The New England Region. RCED-83-36. Washington, DC: 1983.

General Service Administration (hereinafter cited as GSA). Major Information Technology Systems Acquisition Plans of Federal Executive Agencies, 1983-1988. Washington, DC: 1983.

GSA. Catalog and Schedule of Information Resources Management Training. Washington, DC: 1984.

GSA. 1984 Office Automation Survey. Washington, DC: Information Management Assistance Division, Office of Information Resources Management, GSA: 1984.

GSA. End User's Guide to Buying Small Computers. Washington, D.C.: Office of Information Resources Management, GSA: 1984.

Hayes, Robert M., "Politics and Publishing in Washington," Special Libraries, 74(4):322, October 1983.

Hopper, G. Always looking to the future. Government Computer News (3) 9, September 1984.

Horton, Forest Woody. The Information Resource. Information Industry Association. Washington, D.C. 1979.

Hughes, Steve and Janice Rubin, eds. Federal Energy Information Systems and Energy Research and Development Programs. Congressional Research Service, The Library of Congress. Washington, DC: 1975.

Kirchner, Jake. OTA: ADP May Hinder Oversight. Government Computer News, (3) 9, September 1984.

Levin, Marc A., "Access and Dissemination Issues Concerning Federal Government Information," Special Libraries, 74(2):127, April 1983.

Levitan, K.B. 1982. Information Resource(s) Management - IRM. In Martha E. *Williams, ed. Annual Review of Information Science and Technology.* American Society for Information Science. Vol 17. White Plains, N.Y.: Knowledge Industry Publications, Inc. pp.227-266.

Licklider, J.C.R. 1981. Computers and Government. The Computer Age: A Twenty-Year View, p.27. Michael L. Dertouzos and Joel Moses, eds. Cambridge: The MIT Press.

Masuda, Yoneji. 1981. The Information Society as Post-Industrial Society. Tokyo: Institute for the Information Society.

McCorduck, Pamela. 1979. Machines Who Think. San Francisco: W.H Freeman and Co.

Miller, Nancy. Information Resources Management (IRM): An Approach to Implementation of the Paperwork Reduction Act. Congressional Research Service, The Library of Congress, IB81166. Washington, DC: 1984.

Mowshowitz, Abbe. 1976. The Conquest of Will: Information Processing in Human Affairs. Philippines: Addison-Wesley Publishing Co. Inc.

National Bureau of Standards. Computer Science and Technology, NBS Special Publication 500-102. Microcomputers: A Review of Federal Agency Experiences. Washington, DC: 1983.

National Bureau of Standards. Computer Science and Technology. NBS Special Publication 500-84. Costs and Benefits of Database Management: Federal Experience. Washington, DC: 1981.

National Commission on Libraries and Information Science (NCLIS). Annual Report, 1982-1983. Washington, DC: NCLIS, April 1984.

Office of Management and Budget (hereinafter cited as OMB). Improving Government Information Resources Management: A Status Report. Washington, DC: 1983.

OMB/GSA. Office of Information and Regulatory Affairs. Major Information Technology Systems Acquisition Plans of Federal Executive Agencies, 1983-1988. Washington, DC: 1983.

Office of Technology Assessment (hereinafter cited as OTA). A Preliminary Analysis of the IRS Tax Administration System, Washington, DC: Office of Technology Assessment, March 1977, OTA-TCI-43.

OTA. An Assessment of Alternatives for a National Computerized Criminal History System. Office of Technology Assistance. Washington, DC: 1982, OTA-CIT-161.

Pikul, Robert, et al. 1979. Assessment of the Management of Information Processing Activities in the Department of Energy. Vol. II. Detailed Description and Assessment of Information Processing Management Activities. McLean, Virginia: The MITRE Corporation.

Privacy Study Commission. 1977. Personal Privacy in an Information Society. Washington, D.C.: Government Printing Office.

Regan, Priscilla A. Personal Information Policies in the United States and Britain: The Dilemma of Implementation Considerations. Journal of Public Policy 4, 1, 19-38.

Relyea, Harold C. and Elaine R. Tomchik. Managing Official Information—Accessibility and Protection in the Federal Government: A Selected Bibliography. Congressional Research Service, The Library of Congress. Report No. 80-183 GOV. Washington, DC: 1980.

Robertson, Lawrence S. and Robert F. Aldrich. 1981. Dissemination of Information. Issues in Information Policy, National Telecommunications and Information Administration Special Publications. Washington, D.C.: U.S. Department of Commerce, pp. 19-32.

Rosenberg, Victor. 1982. National Information Policies. In Martha E. Williams, ed. Annual Review of Information Science and Technology. Vol. 17. American Society for Information Science. White Plains, N.Y.: Knowledge Industry Publications, Inc.

Rule, James B. 1974. Private Lives and Public Surveillance. Social Control in the Computer Age. NY: Schocken Books.

Saloschin, Robert L., Thomas C. Newkirk, and Donald J. Gavin. A Short Guide to the Freedom of Information Act. Washington, DC: Department of Justice, 1980.

Simon, Herbert A. 1981. In Michael L. Dertouzoz and Joel Moses, eds. The Consequences of Computers for Centralization and Decentralization. The Computer Age: A Twenty-Year View. Cambridge: The MIT Press. pp. 212-228.

Smith, Jean, "Information: Public or Private," Special Libraries, 74(2):275, October 1984.

Struck, Myron, "Old Printery Undergoes a Makeover," The Washington Post, November 8, 1984, p. A25.

Wessel, Andrew E. 1976. The Social Use of Information. Ownership and Access. NY: John Wiley & Sons.

Westin, Alan F. and Michael A. Baker. 1972. Databanks in a Free Society. Computers, Record-Keeping and Privacy. A Project of the Computer Science & Engineering Board, National Academy of Sciences. NY: Quadrangle/New York Times Book Co.

Yurow, Jane H. Issues in Information Policy. NTIA Special Publications. U.S. Department of Commerce, National Telecommunications and Information Administration. Washington, DC: 1981.

ATTACHMENT 1

INTERVIEW PROTOCOL

The KBL Group, Inc.

Attachment 1

INTERVIEW PROTOCOL FOR AGENCY PROFILES

I. BASIC QUESTION FRAMEWORK

1. What are the information practices and procedures of the agency?

   1.1. What personal and/or company information is collected? How is it used?
   1.2. How is public access to agency decisionmaking (both rulemaking and adjudication) provided?
   1.3. How is public information disseminated? Qualitative and quantitative comparison between dissemination activities in 1976 and at present.

2. What technology, if any, is involved in each of the three areas?

   2.1. Categories of technology.
   2.2. How has the use of technology affected agency information practices?

3. What plans, if any, does the agency have to employ new technologies?

4. How have the above practices changed since 1976?

II. QUESTION TOPICS BY OFFICIAL BEING INTERVIEWED

A Public Information/Publications

1.1a Categories of personal/company information collected, if any. (If none collected, following questions apply to information collected by other agency offices but used by this office); from whom collected; for what uses (routine and nonroutine, including matching and profiling); law or policy that mandates collection; non-routine exchanges and disclosures of information: to whom, prerequisites for, and number of instances per year; use of electronic identifier; procedures for ensuring record quality.

1.1b FOIA/Privacy Act requests handled, if any. Number granted or denied out of number of requests.

1.1c Extent and nature of staff training re: sensitivity and privacy of agency records.

1.2a Provision of information/documents necessary for citizen access to agency decisionmaking: Federal Register, reading room or sale (FOIA (1 & 2)).

1.2b Any public notification of hearings, meetings, rulemaking procedures--methods of.

1.3a Number and type of publications published; method of filling requests for documents--reading room, mail order, store in agency; free or sale--if sale, typical cost.

1.3b Marketing--type, amount, any marketing documents.....

1.3c Contracting done with the private sector for information dissemination. Type and numbers of contracts.
1.3d Provision of public access to Inspector General reports, if any.
1.3e Major users of information produced/disseminated.
1.3f Number and type of research studies done, if any. Published in-house or otherwise.
1.3g Educational materials produced; for what audience; number produced; dissemination of educational materials produced by others; what materials and how disseminated--sale, reading room, etc.
1.3h Are instructions published to help constituents fill out forms, etc. Where and how available.
1.3i Criteria for document distribution. Describe distribution decisionmaking process; person responsible.

2. What technology, if any, is involved in each of the three areas?

2.1 Categories of technology.
2.2. How has the use of technology affected agency information practices?

3. What plans, if any, does the agency have to employ new technologies?

4. How have the above practices changed since 1976?

B Information Center/Library

1.1a Categories of personal/company information collected, if any. (If none collected, following questions apply to information collected by other agency offices but used by this office); from whom collected; for what uses (routine and nonroutine, including matching and profiling); law or policy that mandates collection; non-routine exchanges and disclosures of information: to whom, prerequisites for, and number of instances per year; use of electronic identifier; procedures for ensuring record quality.
1.1b Extent and nature of staff training re: sensitivity and privacy of agency records.
1.3a Major users of information disseminated. Extent of public access to collection and to use of other collections via reference service.
1.3b Has use of center/library been stable? If not, why? Note changes if any between 1976 and present and reasons for.
1.3c Extent of contracting with private sector--type of contracts.
1.3d Number and type of publications produced; how disseminated and to whom.
1.3e Marketing--type, amount, to whom.
1.3f Relationship with Records, IRM, Publications and/or Public Information offices.
1.3g Provision of public access to Inspector General reports, if any.

2. What technology, if any, is involved in each of the three areas?

   2.1. Categories of technology.
   2.2. How has the use of technology affected agency information practices?

3. What plans, if any, does the agency have to employ new technologies?

C Inspector General (possible contact person)

   1.1a Current or past investigations which concern agency practices re: collection of personal/corporate information.
   1.1b Collection/use of personal information to investigate agency fraud waste abuse--see A1.1a above.
   1.1c Extent and nature of staff training re: sensitivity and privacy of agency records.
   1.3a Provision of public access to Inspector General reports --procedure and costs.
   1.3b Extent of contracting with private sector for studies--type and use (in semiannual reports or just ongoing investigation); extent to which contracted studies use personal information.

2. What technology, if any, is involved in each of the three areas?

   2.1. Categories of technology.
   2.2. How has the use of technology affected agency information practices?

3. What plans, if any, does the agency have to employ new technologies?

4. How have the above practices changed since 1976?

D Records Manager

   1.1a Categories of personal/company information collected, if any. (If none collected, following questions apply to information collected by other agency offices but used by this office); from whom collected; for what uses (routine and nonroutine, including matching and profiling); law or policy that mandates collection; non-routine exchanges and disclosures of information: to whom, prerequisites for, and number of instances per year; use of electronic identifier; procedures for ensuring record quality.
   1.1b FOIA/Privacy Act requests handled, if any. Number granted or denied out of number of requests.
   1.1c Extent and nature of staff training re: sensitivity and privacy of agency records.
   1.2a as in A above
   1.3a Major users of information collected and disseminated. Extent and means of public access to records.
   1.3b Content and source of record maintained.
   1.3c Relationship with Information Center/Library, Public Information/Publications.
   1.3d Records/publications distributed, if any. Procedure.

1.3e Extent of contracting with private sector for any office functions.
1.3f Provision of public access to Inspector General reports, if any. Procedures and costs.
1.3g Production/publication of materials, if any. Type and amount.

2. What technology, if any, is involved in each of the three areas?

2.1. Categories of technology.
2.2. How has the use of technology affected agency information practices?

3. What plans, if any, does the agency have to employ new technologies?

4. How have the above practices changed since 1976?

E IRM/Technology/DP/Telecommunications
Heaviest emphasis will of course be on areas 2 and 3

1.1a Categories of personal/company information collected, if any. (If none collected, following questions apply to information collected by other agency offices but used by this office); from whom collected; for what uses (routine and nonroutine, including matching and profiling); law or policy that mandates collection; non-routine exchanges and disclosures of information: to whom, prerequisites for, and number of instances per year; use of electronic identifier; procedures for ensuring record quality.
1.1b Completed or ongoing IRM reviews of personal/company data collection procedures; specifics and results, such as burden reduction.
1.1c Extent and nature of staff training re: sensitivity and privacy of agency records.
1.2a Completed or ongoing IRM reviews of procedures allowing public access to agency decisionmaking and to documents connected with decisionmaking; specifics and results, such as improved public access.
1.3a Completed or ongoing IRM reviews of reporting and publication of public information; specifics and results, such as budget savings, efficiency, improved distribution.

2. What technology, if any, is involved in each of the three areas?

2.1. Categories of technology.
2.2. How has the use of technology affected agency information practices?

3. What plans, if any, does the agency have to employ new technologies?

4. How have the above practices changed since 1976?

F Legislative Affairs /Congressional Liaison
Principal use will be a contact, and as a backup when questions are unanswered after interviews with other officials.

4. Describe any agency requests for a change in the laws in any of the above areas.

G General Counsel/Legal Division

1.1a FOIA denials handled--number denied out of number of requests. Involvement, if any, in subsequent litigation.
1.1b Advice/written opinions re: agency collection and use of personal/company information as in A1.1a above.
1.1c Notice of new systems--evaluation of effect on privacy rights; frequency of change and provision of notice.
1.1d Extent and nature of staff training re: sensitivity and privacy of agency records.
1.2a Role in rulemaking--advice of legal consequences, participation in hearings, notifications, findings that notice is not necessary, certifications of closed meetings (number and type).
1.2b Regulatory Impact and Flexibility Analyses.
1.2c FOIA requests see 1.1a above.

2. What technology, if any, is involved in each of the three areas?
2.1. Categories of technology.
2.2. How has the use of technology affected agency information practices?

3. What plans, if any, does the agency have to employ new technologies?

4. How have the above practices changed since 1976?

H Contracts

1.1a Extent of contracting-out of personal/company data collection; number and type.
1.1.b Extent and nature of staff training re: sensitivity and privacy of agency records.
1.3a Extent of contracting-out of information systems and distribution: Library/Information Center functions; agency studies; publications; records; number and type.

I Programs

1.1a Categories of personal/company information collected, if any. (If none collected, following questions apply to information collected by other agency offices but used by this office); from whom collected; for what uses (routine and nonroutine, including matching and profiling); law or policy that mandates collection; non-routine exchanges and disclosures of information: to whom, prerequisites for, and number of instances per year; use of electronic identifier; procedures for ensuring record quality.
1.1b Extent and nature of staff training re: sensitivity and privacy of agency records.

1.3a If agency has no library, was it closed and reasons for closing.
1.3b Extent of contracting-out of information systems and distribution; library functions; agency studies; publications; records; number and type.

2. What technology, if any, is involved in each of the three areas?

2.1. Categories of technology.
2.2. How has the use of technology affected agency information practices?

3. What plans, if any, does the agency have to employ new technologies?

4. How have the above practices changed since 1976?

J FOIA Officer

1.1a Categories of personal/company information collected, if any. (If none collected, following questions apply to information collected by other agency offices but used by this office); from whom collected; for what uses (routine and nonroutine, including matching and profiling); law or policy that mandates collection; non-routine exchanges and disclosures of information: to whom, prerequisites for, and number of instances per year; use of electronic identifier; procedures for ensuring record quality.
1.1b Number of FOIA/Privacy Act requests handled. Number granted or denied out of number of requests.
1.1c Type of information generally sought and by whom.
1.1d What person/office, if any, handles denials and litigation?
1.1e Extent and nature of staff training re: sensitivity and privacy of agency records.

2. What technology, if any, is involved in each of the three areas?

2.1 Categories of technology.
2.2 How has the use of technology affected agency information practices?

3. What plans, if any, does the agency have to employ new technologies?

4. How have the above practices changed since 1976?

K Other Functionaries as relevant to the agency (such as Archivist, Historian), with questions to the Records Manager.

ATTACHMENT 2

INTERVIEWEES

Attachment 2 - Interviewees

DEPARTMENT OF AGRICULTURE

INTERVIEWEE LIST

NAME	TITLE	PHONE
Jane Benoit	Records and Information Manager	447-2118
George Braley	Deputy Administrator, Special Nutrition Programs	756-3052
Virgil Conrad	Deputy Administrator, Family Nutrition	756-3026
Nelson Fitton	Director, Publications, Office of Government Relations	447-6623
June Langford	Special Assistant, Rulemaking	756-3064
Joseph Leo	Deputy Administrator, Management	765-3030
Ann Patrick	Security Officer	--
Eric Mondres	Congressional Liaison	447-7095
Don Morton	Deputy Director, OIRM	447-3152
Robert Sobecki	Technology, OIRM	447-8920
Bob Whiting	Freedom of Information Officer	756-3030
Richard Woods	Director, Government Affairs	756-3012

CONSUMER PRODUCT SAFETY COMMISSION

INTERVIEWEE LIST

NAME	TITLE	PHONE NO.
Steve Butler	Director, Office of Automatic Data Processing	492-6445
Margo DeFerranti	Attorney, Office of the General Counsel	492-6986
Sadye Dunn	Director, Office of the Secretary	492-6800
Elizabeth Goldberg	Chief, Library/Information Services Branch	492-6544
Walter Hobby	Associate Executive Director for Economic Analysis	492-6962
Elizabeth Johnson	Consumer Education Officer, Outreach Coordination Office	492-6580
Nancy Johnson	Director, National Injury Information Clearinghouse	492-6424
Art McDonald	Division Director, Hazard and Injury Data Systems, Epidemiology	492-6539
Judith Pitcher	Division Director, Economic Analysis	492-6962
Todd Stevenson	Freedom of Information Officer	492-6800
Brannon Thompson	Information Resources Management and Security Specialist	492-6854
Dr. Robert Verhalen	Associate Executive Director for Epidemiology	492-6440

DEPARTMENT OF ENERGY

INTERVIEWEE LIST

NAME	TITLE	PHONE
Elizabeth Buffum	Associate Manager, Office of Scientific and Technical Information	252-8842
Linda Carlton	Deputy Assistant, General Counsel for General Law	252-8618
Bruce Dwyer	Director, Planning and Evaluation Division, Energy Information Administration	252-6463
Robert Greeves	Director, Office of ADP Management	353-4720
Paula Hill	Chief, Business Information Systems Branch, Information Systems Division, Office of Computer Services and Telecommunications Management	353-2856
Jack Hall	Chief Historian History Division/Archives	353-5431
Albert Linden	Deputy Administrator Energy Information Administration	252-6351
Otto Reid	Director, Management Information System, Office of Hearings and Appeals	252-6622
Ron Turner	Director Reference and Information Division	252-5955
William Vitale	Director, Execution Secretariat	252-5230
Kathy Weigl	Energy Information Administration	252-6463
Charles Wrenn	Security Officer, Office of Computer Services and Telecommunications Management	353-4633

OTA - IRS Briefing

December 13, 1984 (A.M.)

Beck, Alan	IRS, PM:S	566-9483
Bergman, Walt	IRS, PM:PFR	566-9497
Broder, Margo L.	IRS, CC:D	566-3074
Carvey, Ed	IRS, PM:S:FM	566-3111
Endick, Stuart	IRS, CC:GLS	566-3566
Farbenblum, Marcus	IRS, P:DS:P	535-4179
Joseph, Sommers	IRS, PM:S:DS:S	535-9437
Layel, Ron	IRS, PM:S:FM:O	566-9094
Levitan, Karen	KBL	588-4633
Moore, Frank	IRS, PM:S:FM:S	535-4239
O'Brien, Ray	IRS, PM:S:FM:O	566-9711
Persky, Tom	IRS, C	566-4071
Regan, Priscilla	OTA	226-2170
Rudd, Derle	IRS, I	566-3743
Taggart, David	IRS, PM:S:FM:T	376-0521
Tiffany, Tom	IRS, C:L	566-3157

Arthur Altman	Director, Tax Forms and Publications	566-6150
Kirk Markland	Online Publications	566-6154
Tom May	Director, Publications Services	566-3873

OTA - IRS Briefing

December 13, 1984 (F.M.)

Broder, Margo	IRS, CC:D	566-3074
Gibb, Charles	IRS, CP:CI:P	566-4554
Levitan, Karen	OTA	588-4633
O'Brien, Ray	IRS, PM:S:FM:O	566-9711
Persky, Tom	IRS, C	566-4071
Pope, Jean	IRS, OP	566-4641
Regan, Priscilla	OTA	226-2170
Tiffany, Tom	IRS, C:L	566-3157
Wauben, Bill	IRS, OP:C	566-4380
Williams, Fred	IRS, C	566-4143

OTA - IRS Briefing

December 14, 1984

Barbato, Gene	IRS, D:C:H:C	756-6301
Barth, Patricia	KBL	588-4633
Broder, Margo L.	IRS, CC:D	566-3074
Capozzoli, Daniel N.	IRS, D:C	566-4009
Karlsen, Marge	IRS, D:C:S:I	566-6930
Laycock, Thomas J.	IRS, D:C	566-4007
Layel, Ron	IRS, PM:S:FM:O	566-9094
Martin, Thomas	IRS, D:R:T	566-6811
Neal, Ken	IRS, D:C:R	566-6936
Persky, Tom	IRS, C	566-4071
Regan, Priscilla	OTA	226-2170
Russo, Philip P.	IRS, D:R:T	566-6252
Scheureai, Fritz	IRS, D:R:C (D:R:S)	376-0216
Schorr, Barry	IRS, D:R:P	566-4721
Stalcup, Steve	IRS, D:R:R	566-6883
Strutko, John	IRS, PM:HR:MIS	566-4816
Tiffany, Tom	IRS, C:L	566-3157

DEPARTMENT OF LABOR

INTERVIEWEE LIST

NAME	TITLE	PHONE NO.
Tom Burn	Director, Office of Information Resource Management (ETA)	
John Dineen	Director, Information Technology (OASAM)	523-1687
Russell Flanders	Executive Director, National Occupational Information Coordinating Committee (ETA)	653-5665
Carolyn Golding	Director, Unemployment Insurance (ETA)	376-6636
Tom Komarek	Assistant Secretary for Administration and Management (OASAM)	523-9086
Donald Lemmon	Director, Management Policy and Systems (OASAM)	523-6073
Robert Litman	Employment Service (ETA)	376-6750
Vernon Louviere	Director, Office of Information and Public Affairs	523-9711
Janice Sawyer	Administrator, Office of Financial Control and Management Systems (ETA)	376-6585
David Williams	Office of Program and Fiscal Integrity (ETA)	376-2022

SMALL BUSINESS ADMINISTRATION

INTERVIEWEE LIST

NAME	TITLE	PHONE
Lawrence E. Barrett	Chief, Information Systems Branch, Office of Computer Sciences	653-6463
John Bjork	Security Program Manager, Audit and Investigations Division of Inspector General's Office	653-6355
Angelique Butler	Information Specialist, Office of Information for the Office of Advocacy	634-7611
Carman Celucci	Chief, Administrative and Accounting Section, Office of Computer Sciences	653-2058
Gregory Diercks	Writer/Editor Management Assistance	653-6634
Michael J. Dowd	Chief, Financial Division, Washington District Office	634-4802
Ann H. Glascock	Chief, Data Base Administration Staff, Office of Computer Sciences	653-6738
Margaret M. Hickey	Librarian Small Business Information Staff	653-6914
Al Jones	Chief, Portfolio Management Division, Washington District Office	634-4975
Nicholas Kalcounas	Administrative Judge/Director of Freedom of Information and Privacy Act Appellate Office	653-6460
Blake Kingsley	Staff Assistant, Office of Public Communication	653-6822
David R. Kohler	Acting Associate General Counsel for General Law	653-6660

Richard P. Lewis	Computer Systems Analyst, Information Systems Branch, Office of Computer Sciences	653-6738
Grant G. Moy, Jr.	Special Assistant to the General Counsel	653-6642
Dwight Reynolds	Computer Security Officer	653-2073
Patrick Stiehm	(Formerly) District Counsel Washington District Office, (Now) Trial Attorney, Office of General Counsel	653-6660
John J. Sweeney	Deputy Associate Administrator for Management Assistance	653-6330
Paul G. Swope	Director, Office of Computer Sciences	653-6708
Marty Teckler	Deputy General Counsel, Office of Legislation	653-6660
Robert A. Turnbull	Associate Deputy Administrator for Resource Management	653-6431
Elizabeth Zaic	Chief, Information Resources Management Branch	653-8538

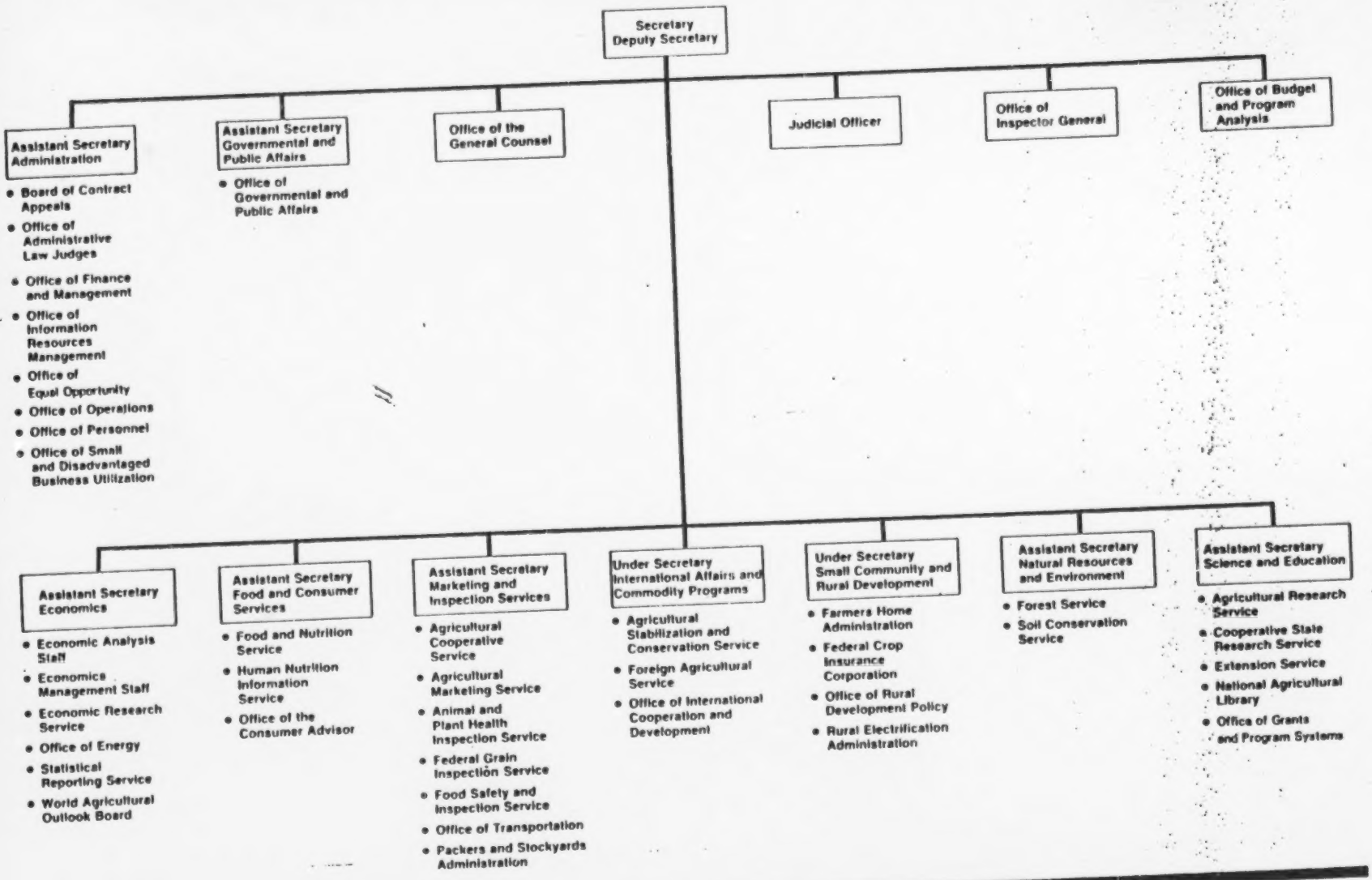
VETERANS ADMINISTRATION

INTERVIEWEE LIST

NAME	TITLE	PHONE NO.
Strat Appleman	Executive Assistant to Associate Deputy Administrator for Public Affairs	389-2818
Roy Bailey	Deputy Director for Administrative Services, Department of Veterans Benefits	389-2744
Doug Bartou	Attorney, Office of the General Counsel	389-3688
Russ Bowman	Publications Management Staff, Chief, Department of Medicine and Surgery	389-2258
Esther Georgatos	Director, Information Technology Center	389-5524
Allan Gohrband	Associate Director for ADP Policy and Operations Management	389-5164
Harold Gracey	Executive Assistant Associate Deputy Administrator for Information Resources Management	389-5333
Edward D. Green	Director, Veterans Assistance Service, Department of Veterans Benefits	389-2567
Clarence Johnson	Systems Security Officer Department of Veterans Benefits	389-3461
John Kleine	Deputy Assistant General Counsel Office of the General Counsel	389-3007
Marjorie M. Llandri	Chief, Records Management Division	389-3616
Cicely Marks	Senior Technical Services Specialist, Library Division	389-5130
Nancy McCoy	Chief, Directives Management Division	389-3616

Jean McVoy	Resources Coordination Specialist, Library Division	389-2430
Ren Morani	Deputy Inspector General	389-3461
Larry Nicholson	Chief, Directives Staff Compensation and Pension Service Department of Veterans Benefits	389-3062
Robert Oakley	Assistant Inspector General for Auditing	389-2627
Karen Renninger	Chief, Library Division	389-2711
Robert Schultz	Director, Office of Information Management and Statistics	389-2423
Mary Ann Tatman	AV Program Specialist Library Division	389-5130

United States Department of Agriculture


Secretary
Deputy Secretary
Assistant Secretary Administration
• Board of Contract Appeals
• Office of Administrative Law Judges
• Office of Finance and Management
• Office of Information Resources Management
• Office of Equal Opportunity
• Office of Operations
• Office of Personnel
• Office of Small and Disadvantaged Business Utilization
Assistant Secretary Governmental and Public Affairs
• Office of Governmental and Public Affairs
Office of the General Counsel
Judicial Officer
Office of Inspector General
Office of Budget and Program Analysis
Assistant Secretary Economics
• Economic Analysis Staff
• Economics Management Staff
• Economic Research Service
• Office of Energy
• Statistical Reporting Service
• World Agricultural Outlook Board
Assistant Secretary Food and Consumer Services
• Food and Nutrition Service
• Human Nutrition Information Service
• Office of the Consumer Advisor
Assistant Secretary Marketing and Inspection Services
• Agricultural Cooperative Service
• Agricultural Marketing Service
• Animal and Plant Health Inspection Service
• Federal Grain Inspection Service
• Food Safety and Inspection Service
• Office of Transportation
• Packers and Stockyards Administration
Under Secretary International Affairs and Commodity Programs
• Agricultural Stabilization and Conservation Service
• Foreign Agricultural Service
• Office of International Cooperation and Development
Under Secretary Small Community and Rural Development
• Farmers Home Administration
• Federal Crop Insurance Corporation
• Office of Rural Development Policy
• Rural Electrification Administration
Assistant Secretary Natural Resources and Environment
• Forest Service
• Soil Conservation Service
Assistant Secretary Science and Education
• Agricultural Research Service
• Cooperative State Research Service
• Extension Service
• National Agricultural Library
• Office of Grants and Program Systems

U.S. DEPARTMENT OF AGRICULTURE
WASHINGTON, D.C. 20250

DEPARTMENTAL REGULATION	NUMBER: 3130-2
SUBJECT: Microcomputer Policy	DATE: May 24, 1984
	OPI: Agency Technical Services Division Office of Information Resources Management

1 PURPOSE

This regulation establishes policy and requirements for the acquisition and operation of microcomputers in USDA in order ~~to assure effective~~ application of advanced technology.

The purpose of this regulation is to achieve a balance between orderly growth and uncontrolled adoption of the latest and most attractive technological features.

2 CANCELLATIONS

This regulation supersedes DR 3130-2, Microcomputer Policy, dated December 20, 1982.

3 POLICY

It is USDA policy to acquire, through planned and consolidated lease or purchase, cost effective, compatible microcomputer systems throughout the Department and to manage these resources efficiently.

Microcomputers intended to support a function or application common to many agency units must be acquired through consolidated lease or purchase, even though installation of all equipment may not be concurrent.

The Department encourages agencies to experiment, to share information and other resources, and to maximize communication among agencies.

To assure orderly microcomputer systems acquisition, it is USDA policy that agencies will:

a Standardize equipment and software agency-wide and consolidate acquisitions;

b Perform requirements, feasibility, and cost-benefit studies consistent with the size and complexity of each acquisition;

c Establish a correlation between agency acquisition plans and actual acquisitions;

DISTRIBUTION: 31

d Restrict applications software, to the maximum extent possible, to commonly-available, off-the-shelf packages.

USDA microcomputer policy will be evaluated annually.

4 REPORTS

a Planning. Agency intent to acquire microcomputers will be discussed in the agency Long-Range IRM Plan and detailed in Exhibit 43-B of the agency's annual OMB A-11 submission.

b Performance. By December 31 of each year, agencies will submit to the Director, OIRM, a narrative statement which provides the number, models, and acquisition costs of microcomputers acquired during the previous fiscal year and correlates them to those estimated in the agency's A-11 budget submission. Agencies shall use the Departmental Information Locator System to maintain an inventory of acquired microcomputers.

5 DEFINITIONS

a Agencies. USDA agencies and staff offices.

b Instrumentation Systems. Those systems which are used in conjunction with or to control laboratory instruments or equipment such as gas chromatographs or mass spectrometers.

c Microcomputer. One of a variety of general purpose computers manufactured utilizing one or more microprocessors. Microcomputers can range from computers with relatively small amounts of memory to computers with large amounts of random access memory and several peripheral devices. They normally require no special environmental site preparation. They are often called personal, professional, or end user computers.

d Process Control Systems. Those systems used for real-time regulation of physical processes or reactions in either laboratory or production situations.

e Sensitive Systems. Systems which process national security, personal, financial, proprietary, or market-sensitive data; systems which are time-critical; systems which affect life-critical situations; systems which have a significant impact on agency operations; or systems whose reconstruction would be difficult or expensive.

6 REQUIREMENTS FOR ACQUISITION

a Agencies will conduct requirements, feasibility, and cost-benefit studies commensurate with the size and complexity of each proposed system; documentation will be maintained in agency files for inspection. These studies will include security considerations.

b Agencies will standardize microcomputer equipment and software agency-wide.

c Microcomputers acquired will use at least one of these operating systems in normal day-to-day operations:

CP/M, MS-DOS, PC-DOS, or UNIX

and, if program development is required, support one or more of the following standard languages: COBOL, FORTRAN, BASIC, PASCAL, ADA, and C.

Scientific and research systems which are used primarily for analysis of data (whether or not collected by instrumentation or process control systems) are excluded from the requirements of Sections 6 b, 6 c, and 7 b; instrumentation and process control systems are also excluded from these requirements. An agency which has a need for these systems will submit for OIRM approval, justification for the variance from the standardization requirements. However, agencies should strive for standardization of these special-purpose systems and consolidate purchases when possible.

d Microcomputers acquired to be used in telecommunications mode must be compatible with the Departmental Network (DEPNET). Establishment of local area networks requires OIRM approval.

Interactive communicating microcomputers must be capable of using the asynchronous ASCII (TTY) protocol or the synchronous IBM 3270 protocol. Microcomputers used for remote batch processing must be capable of using IBM 2780/3780 protocol.

Federal Standard 1041 (CCITT X.25) is a communications protocol which is usually implemented on communications links only. This protocol is supported by DEPNET and is transparent to the terminal user. X.25 is now being integrated into microcomputer architecture. OIRM urges agencies to acquire this feature; X.25 will then be used in concert with (as a super set of) the protocols listed above.

7 OPERATING STANDARDS

a If microcomputers are used in a telecommunications environment, security requires special, strict safeguards. Sensitive systems shall not be installed in a microcomputer network unless adequate software is acquired or developed and adequate procedures are established to provide the requisite security. Examples of controls which may be used are:

(1) Designating one computer to manage the network through use of access control and logging software.

(2) Data encryption.

b Application software will, to the maximum extent possible, consist of commonly-available off-the-shelf packages. Applications which must be developed must be programmed in one of the languages listed in Section 6 c. Agencies must exercise strong central control over application development, maintenance, and change to assure standards adherence and compatibility and to curtail redundant efforts. Agencies should freely exchange information and share software whenever possible.

8 OPERATIONAL CONTROLS

a Commercially-available software is usually copyrighted, and all rights are reserved to the copyrighter. This means that any copying, duplicating, selling, or other distribution of the software for other than backup use by the lawful users of the software is a crime. Commercially-available software which is copyrighted generally may only be entered or its copy entered from the storage medium into the computer and executed by the lawful user. Willful violations of the Copyright Law of the United States can result in civil damages of up to $50,000 in addition to actual damages, plus criminal penalties of up to one year imprisonment and/or a $10,000 fine. Agencies must inform employees that USDA strictly forbids violation of copyrights.

b Agencies must establish a means to manage ADP data, computer software, and related files effectively in a microcomputer environment. This includes controlling these items to establish ownership and sensitivity, to determine which copy is the "official" one, and to assign and execute responsibility for access control management, use, disclosure, updating, and disposition. Controls for retention of ADP data, software, and related files shall comply with the agency requirements for records management, or, in absence of those, comply with the Federal General Records Schedule 20.

c Agencies will insure that continuity of operations, when involving microcomputers, is planned for in event of disaster, employee death or separation from employment with USDA, or other situation. Requirements for security of ADP operations shall be met.

9 TECHNICAL APPROVAL THRESHOLD

a An agency may acquire microcomputers without OIRM technical approval when the system life cost of the equipment, software, training, telecommunications and maintenance items is less than $100,000 ($50,000 non-competitive) purchase or $3,000 monthly rental or lease in any acquisition or as required by DR 3130-1, Technical Approvals.

b When this threshold is to be exceeded in any one planned, consolidated acquisition, the requirements of DR 3130-1 apply. A brief narrative statement that makes a connection between the proposed acquisition and the agency A-11 estimates will be provided with the DR 3130-1 requirements.

-END-

ATTACHMENT 4

ENERGY PROGRAM MATERIAL

The KBL Group, Inc.

FACTS EVERY DOE ADP USER SHOULD KNOW ABOUT THE PRIVACY ACT OF 1974

FACTS EVERY DOE ADP USER SHOULD KNOW ABOUT THE PRIVACY ACT OF 1974

1. **Question** - What is the Privacy Act of 1974?

   Answer - The Privacy Act of 1974 (Public Law 93-579), is a Federal Statute enacted by the U. S. Congress to protect the rights of individuals.

2. **Question** - Why was the Privacy Act needed?

   Answer - The United States Congress found that;

   a. The privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by federal agencies;

   b. The increasing use of computers and sophisticated information technology, while essential to the efficient operations of the government, has greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use, or dissemination of personal information;

   c. The opportunities for an individual to secure employment, insurance, and credit, and his right to due process, and other legal protections are endangered by the misuse of certain information systems;

   d. The right to privacy is a personal and fundamental right protected by the Constitution of the United States; and

   e. In order to protect the privacy of individuals identified in information systems maintained by federal agencies, it is necessary and proper for the Congress to regulate the collection, maintenance, use, and dissemination of information by such agencies.

3. **Question** - What is the purpose of the Act?

   Answer - The purpose of the Act is to provide certain safeguards for an individual against an invasion of personal privacy by federal agencies.

4. **Question** - What are the safeguards mentioned above and what does the Act require each federal agency to do?

Answer -

a. Permit an individual to determine what records pertaining to him are collected, maintained, used, or disseminated by such agencies;

b. Permit an individual to prevent records pertaining to him obtained by such agencies for a particular purpose from being used or made available for another purpose without his consent;

c. Permit an individual to gain access to information pertaining to him in federal agencies' records, to have a copy of all or any portion thereof, and to correct or amend such records;

d. Collect, maintain, use, or disseminate any record of identifiable personal information in a manner that assures such action is for a necessary and lawful purpose, that the information is correct and accurate for its intended use, and that adequate safeguards are provided to prevent misuse of such information;

e. Permit exemptions from the requirements with respect to records provided in the Act only in those cases where there is an important public policy need for such exemptions as has been determined by specific statutory authority; and

f. Be subject to civil suit for any damages that occur as a result of willful or intentional action that violates any individual's rights under this Act.

5. **Question** - What is Privacy or Personal information?

Answer - Personal information is any information that identifies, describes, or represents characteristics or circumstances directly relatable only to one person. Some examples are: academic history, arrest history, biographical history, criminal history, dental and medical history, educational history, employment history, financial history, history of political activities, religious activities, Social Security Account Number, symbolic identification or code, fingerprints, voice prints, photographs, profiles (dossier), and more.

6. **Question** - What information is not considered personal and privacy information?

Answer - Employee name, grade, step, salary, duty station, and titles past and present.

7. **Question** - What causes a computer application to be subject to the Privacy Act?

   Answer - The fact that the application (system of records) processes files (a collection of records) that contain personal information, and that the records are retrieved or retrievable by some personal identification, such as name, Social Security Account Number, or any other identifying number, symbol, or other identifying particular assigned to an individual, causes the application to be subject to the Act.

8. **Question** - How is access to personal information controlled at DOE?

   Answer - Access to personal information is controlled by limiting access to those employees whose job requires access, such as people working in Personnel, Payroll, supervisors, secretaries, public health officers, etc. (those with the need to know). In the ADP environment, there are access lists, computer access control software packages such as "Access Control Facility 2", data base passwords, etc.

9. **Question** - How is personal information protected in the ADP environment, the office automation environment?

   Answer - Personal information is protected by;

   a. Controlling access to files, reports, magnetic tapes, and disks;

   b. Printing or stamping "Personal Information" or "Privacy Information" on computer output reports, and by using a "P" in the 20th position of the programmer name field on a job card or card image. This will cause "Personal Data" to be printed on the cover sheets of computer output printed in the Computer Center;

   c. Using available warning signs (form DOE/DP-0018), which will indicate a number of types of sensitive information, personal information among them. These signs have been designed to be placed on or near terminals or workstations to warn persons entering your office that you are processing sensitive information;

   d. Keeping printed matter containing personal information in a locked container or locked room when not being used;

   e. Labeling magnetic storage media such as tapes, disks, diskettes, and cassettes "Personal Information;

   f. Keeping magnetic storage media containing personal information in a locked container or locked room when not being used.

10. **Question** - What must be done with printed matter containing personal information when it is no longer needed?

Answer - Printed matter containing personal information must be destroyed by shredding or burning. The Headquarters guard force will, on request, collect and supervise the proper destruction of printed matter containing personal information.

11. **Question** - How is personal information that is recorded on magnetic storage media disposed of when it is no longer needed?

Answer - Personal information on magnetic storage media must be erased or completely overwritten (the entire tape or disk) before the tape or disk is reused. This will eliminate the chance of information remaining on the end of a tape or disk if the new file is shorter than the previous one.

12. **Question** - Are there any penalties for not protecting personal information or for violating any of the requirements of the Privacy Act?

Answer - Failure to provide adequate protection for personal information is a violation of the Act, and is a misdemeanor and if found guilty you can be fined not more than $5,000.00 and serve a year in prison.

13. **Question** - What other actions are violations of the Privacy Act?

Answer - Privacy Act violations include;

a. Unauthorized access to, maintenance or disclosure of personal information;

b. Creation and maintenance of a 'System of Records' without satisfying the required publication of a notice in the Federal Register;

c. Willfully requesting or obtaining under false pretenses any record concerning an individual from an agency.

For more information about the Privacy Act, you may call the Computer Protection Program Manager, MA-254.1, 353-4633.

Agenda Item 2B

PROGRESS REPORT: DEVELOPMENT OF EIA CONFIDENTIALITY LEGISLATION*

Presented by: Kathleen R. Weigl
Office of Planning and Resources
Energy Information Administration

INTRODUCTION

This paper is a progress report concerning the Energy Information Administration's (EIA's) efforts to amend current data sharing laws. EIA is seeking the authority to protect proprietary information, gathered for statistical purposes, from disclosure beyond EIA. A second goal is the ability to pledge confidentiality in order to acquire information from other agencies . This issue has been discussed in the past at Committee meetings; it remains a high priority within EIA. EIA would appreciate the Committee's thoughts, particularly from the perspective of the newer members who have not reviewed earlier efforts. The major issues addressed are the conditions for sharing being contemplated, and the criteria for determining which information will classified as "solely for statistical purposes."

BACKGROUND

The EIA was created by the Department of Energy Organization Act (DOEOA), and was granted broad data collection authorities, some of which were inherited from predecessor agencies such as the Federal Energy Administration and the Federal Power Commission. These authorities permit the EIA to serve two different but related purposes. First, the EIA collects data required for analyses of energy issues and for the formulation of energy policy. Aggregate data are generally sufficient for these purposes, and access to individually identifiable data is usually not required. Frequently, statistical sampling techniques can be used, with considerable savings and reduced respondent burden to obtain highly reliable aggregate data. Second, the EIA collects data required for regulation and other specific program uses, such as contingency planning. Data for these purposes are usually collected on a comprehensive company-by-company basis, since individual firms are the focus of interest in assuring compliance with laws and regulations, and for conducting emergency planning.

---

* This is a working document prepared by the EIA in order to solicit advice and comment on statistical matters from the American Statistical Association Committee on Energy Statistics. This topic will be discussed at the meeting to be held on October 27-28, 1983.

Centralizing the collection of both statistical/analytical data and non-statistical/regulatory data in a single Federal agency has raised a number of important and challenging issues. Most of the issues arise from statutory requirements governing the sharing of EIA data with other components of the Department of Energy (DOE) and with other Federal agencies.

Sections 205(f) and 407(a) of the DOEOA require that information in the possession of the EIA be shared, upon request, with other components of the DOE, including the Federal Energy Regulatory Commission (FERC). This requirement means that any data collected or maintained by the EIA, including data collected on a sample basis, must be provided on a company-specific basis to all other entities within the DOE, including those with regulatory functions, if asked.

These disclosure requirements make the EIA unique among Federal statistical agencies. The Census Bureau and the Bureau of Labor Statistics (BLS), for example, routinely promise confidentiality, sometimes with the force of law, to most of their respondents. There are, however, compelling arguments to support a case for interagency disclosure of EIA data. Many other Federal agencies have sought individually identifiable information from EIA to perform both regulatory and analytical functions. In both instances, EIA first attempts to find a way to meet the requirement with aggregate data. At times however, the aggregate statistics are not sufficient. Examples include comparisons of EIA data to data collected directly by the agency to check reporting accuracy, analyzing market behavior in specific, localized aread, and researching regional and local economic issues. In these instances, aggregates do not provide the level of detail required to complete the studies adequately. EIA has cooperated in these efforts where possible to help foster improved analysis. Requests for data to be used directly in legal proceedings have diminished recently, with the EIA emphasis on use of aggregated data, EIA requirements that respondents be notified of the disclosure, and limitations on subsequent uses. However, when an agency can meet EIA limitations, information is provided.

At the same time, however, the disclosure requirements to which the EIA is subject can cause a number of difficulties for a statistical agency. Among these are:

- Companies or other individuals surveyed by the EIA who know that the information they provide may be shared with regulatory agencies may tend to respond more slowly and more cautiously to data questionnaires. Data professionals agree that there is a significant difference in the quality of data collected with assurances of confidentiality and that of data collected without such assurances. Candid response about behavior or intentions are less likely, and respondents may take legal action to delay or avoid submitting their responses. Not only does the quality of the statistical data suffer, but a lower rate of response to voluntary surveys is also likely.

- The EIA is unable to obtain lists of potential survey respondents from other statistical agencies. The Census Bureau and the BLS have been developing and refining their lists or "frames" over decades. These frames encompass many types of energy-related operations, and would be of considerable value to the EIA. However, since these agencies are bound by law or historical precedent to maintain both the confidentiality of their data and the lists they use to collect them, they are unable to share their frames with the EIA because the EIA cannot agree to keep the frames confidential, thus, EIA foregoes a potential for savings and improved lists.

- It is unfair to respondents in a statistical sample to provide their response to a regulatory body while similarly situated businesses avoid the regulators' scrutiny because they were not part of the sample.

The EIA has imposed conditions for access to its data through the implementation of the "DOE Policy on Disclosure of Individually Identifiable Energy Information in the Possession of the EIA" (45 Fed. Reg., 59812). However, this policy does not allow adequate protection for statistical information.

The Office of Management and Budget (OMB) is preparing a government-wide legislative proposal designed to provide more consistent sharing and protection for data maintained by the Federal Government (see agenda item 2A). However, EIA's role as an information agency (as distinguished from a statistical agency) would not allow EIA to participate fully in the OMB program to protect statistical information or obtain information from another statistical agency for a statistical purpose, such as frames development or validation.

LEGISLATIVE PROPOSAL

To resolve this disclosure dilemma, EIA has proposed a legislative remedy. The "EIA Amendments of 1981" legislative proposal was introduced in May 1981 as S. 1281. That proposal would have designated certain information collected by EIA as statistical and protect it from non-statistical uses, and amended several sections of law to allow the Administrator to provide agencies with a binding assurance of non-disclosure in order to obtain statistical information. It also would have eliminated several mandatory reporting requirements. That proposal was not acted upon during the 97th Congress. A new reports proposal, the "EIA Reports Reduction Act" was submitted to Congress in April 1983. A new proposal, the "EIA Amendments," dealing with confidentiality is in preparation.

The "EIA Amendments" is the same in principal, but somewhat different in procedure, as its predecessor. It would add two new subsections to section 205 of the DOEOA. The first subsection

would allow the Administrator to designate certain information as "solely for statistical purposes." Information so designated would be released only under very limited circumstances and dependent upon the requestor. These are shown on the following Table. Data gathered of other than statistical purposes would continue to be treated according to existing law and policy, i.e., carefully controlled inter-governmental sharing for any lawful purpose.

CONDITIONS UNDER WHICH INDIVIDUALLY IDENTIFIABLE INFORMATION GATHERED FOR STATISTICAL PURPOSES MAY BE DISCLOSED

Requestor	Conditions
DOE Office, other Federal Agency, State agency, Congress, Congressional Committee, Congressional Agency	- required to carry out lawful duties and responsibilities; - will be used solely for statistical purpose; - no recontact with submitters of the data; and, - will not be redisclosed in an individually identifiable form.
Inspector General or General Accounting Office	- to be used only for program evaluation or audit related to the specific data collection program, and authorized by law; - will not be used in any legal proceeding other than against EIA; - will not be redisclosed in an individually identifiable form; and, - no recontact with submitters of the data will be allowed.
Court Order, Summons or Subpoena	- to assist prosecution of disclosure violations only; and, - not to be redisclosed in individually identifiable form.

DOE investigation authorities	- for investigation or prosecution for false response or nonresponse;
	- only for proceeding against person charged with failure to respond or false response; and,
	- no redisclosure in an individually identifiable form.
Person to whom data pertains - heir, successor, or agent	- pursuant to a written request from or on behalf of the respondent.
National Archives	- for permanent storage.
Public	- disclosure prohibited

These provisions are designed to satisfy legitimate requirements for disclosure while providing adequate protection for proprietary statistical information. Can the Committee direct EIA to any further situations which should be included, or caveats which should be added?

A second new subsection applies to information maintained by another Federal agency. In those instances in which the sponsoring agency is prohibited from releasing data without an agreement precluding further disclosure, the Administrator would be authorized to enter into a binding assurance of nondisclosure. This binding assurance would preclude any further disclosure by EIA and would allow EIA to refer all requests for the information, including those under the Freedom of Information Act, to the originating agency.

Other provisions include penalties for violation of the subsections and technical corrections to other related provisions.

The newly drafted EIA Amendments proposal incorporates many of the concepts embodied in the OMB omnibus legislation and is consistent with the Spring 1983 proposal, yet was written to stand alone, so that it can seek its way through the legislative process on its own.

IMPLEMENTATION

The critical element in the proposed legislation is designation of information as "solely for statistical purposes." Once designated, the information could not be used for any other purpose. Therefore, it is essential that designation criteria are neither overly liberal, (conceivably forcing dual collection for both statistical and nonstatistical uses) or so conservative that no data series could qualify. Criteria currently under consideration are:

1. Traditional treatment of the data. Information that is traditionally made public would be excluded from this category, as the protections are unnecessary.

2. Sponsorship. Many EIA data collections are sponsored by other DOE elements. In all likelihood, these collections would not be considered "solely for statistical purposes," unless the sponsoring office has statistical needs only.

3. Prior uses of the data. For information which has been gathered in the past, all uses will be explored. For any nonstatistical uses, EIA would determine whether the user could meet its requirements using statistical aggregates.

Can the committee suggest additional criteria?

SUMMARY

The legislative proposal to improve EIA's ability to protect statistical information from inappropriate uses and expand EIA's ability to obtain protected information for statistical uses from other agencies. While this change may complicate EIA's data service function, that complication will be more than offset by the potential for increased sharing of statistical information and improving the integrity of EIA's survey frames.